DOI: 10.62897/COS2025.3-1.14

10-12, November 2025, Győr

DYNAMIC MULTI-HASH CRYPTOGRAPHIC ENGINE ON ZYNQ FPGA FOR ENERGY-CONSCIOUS EDGE AI APPLICATIONS

Abdulmunem A. Abdulsamad*, Sandor R. Repas[a]

*Department of Electrical Engineering and Infocommunications, Széchenyi István University, Győr, Hungary

abdulsamad.abdulmunem@sze.hu

With the increasing demand for energy-efficient edge computing, maintaining secure data processing without sacrificing performance has become a critical requirement. The proposed system introduces a flexible cryptographic engine implemented on the Zynq-7000 FPGA, capable of supporting multiple hashing algorithms, including SHA-2, SHA-3, SHAKE, and BLAKE2, within a unified hardware architecture. The proposed system introduces runtime adaptability, allowing dynamic selection of the most suitable hashing algorithm based on current workload conditions. This eliminates the need for hardware reconfiguration and enhances system flexibility in real-time applications. The design incorporates energy-aware techniques such as clock gating and partial reconfiguration, while a control-driven finite state mechanism manages transitions between operating modes to achieve an effective balance between performance and power consumption. Experimental validation confirms that the system achieves throughput up to 1.25 Gbps while maintaining power consumption below 1 W. Under low-power operating conditions, the design demonstrates energy savings exceeding 40 % compared to conventional static implementations. The proposed architecture provides a scalable and sustainable solution for secure data processing in edge computing environments, particularly in applications requiring real-time adaptability and efficient resource utilisation.

1. Introduction

Emerging modern edge computing platforms not only require data to be processed within a certain time period but also require high security assurances. In these resource-limited environments, low latency and energy efficiency are crucial. However, off-the-shelf software hashing solutions become infeasible. Due to the role of SHA-2 and SHA-3 as cryptographic hash functions, they inevitably involve high computational cost, which is more detrimental to general-purpose processors, especially in embedded systems with limited resources (Sideris et al., 2020; NIST, 2015).

However, general trends towards implementing FPGA-based accelerators have proved that these issues can be solved, allowing for better performance and energy savings. And yet, implementations of MD4 and other hashing algorithms are typically for a specific algorithm and not adaptable to applications with dynamic requirements. As such, they are less applicable for scenarios where the workload can change over time, or where the security requirements can be time-varying as well.

In order to overcome this limitation, this work provides a flexible and fully programmable reconfigurable cryptographic engine mapped on the Zynq-7000 FPGA platform. An architecture to implement a proposal that takes advantage of both online and offline hashing schemes that support various hashing standards in one architecture and are able to adapt themselves based on the operational situation. This is important because many edge AI use cases require some level of flexibility, e.g., privacy-preserving applications like secure medical diagnosis, encrypted machine learning, and robust sensor data transmission. By combining energy-aware design with adaptability, the proposed approach contributes to the efficiency and long-term sustainability of the system in changing security environments.

2. Related work

Many implementations of cryptographic hash functions on FPGAs have been proposed to improve performance and reduce power consumption in embedded system applications (Sideris et al., 2020). Initial work mainly focused on Keccak, the basis of SHA-3, optimising it through pipelining techniques and parallel processing (NIST, 2015). Sideris et al. (2020) demonstrated a high-throughput implementation of the Keccak hash function using FPGA-based architectures. Similarly, El Moumni et al. (2019) showed that SHA-3 hardware implementations achieve significantly higher throughput compared to software implementations. Subsequent work investigated optimised hardware designs to develop high-speed cryptographic processors (Xiong et al., 2024).

Kahri et al. (2016) introduced a pipelined FPGA-based Keccak processor, achieving significant throughput improvements. Recent work by Dolmeta et al. (2023) analysed the performance of various SHA-3 implementations and highlighted trade-offs between performance, resource utilisation, and power consumption. Besides performance improvement, recent research has also focused on energy efficiency and hardware reconfigurability (Zhang et al., 2022). Zhang et al. (2022) proposed an energy-efficient cryptographic accelerator for IoT systems, demonstrating the benefits of hardware-level optimisation.

However, most existing designs adopt a single-algorithm approach, which limits adaptability in dynamic environments (Dolmeta et al., 2023). To address this limitation, this work proposes a reconfigurable multi-hash cryptographic engine capable of supporting multiple algorithms and enabling runtime adaptability for edge AI and energy-constrained applications.

3. Motivation and objectives

The ever-increasing need for secure and effective data analysis and processing in mission-critical environments has driven the adoption of edge computing systems for analysis and processing in healthcare, autonomous technologies, and smart infrastructure. Because of the high degree of power and latency locking that these systems are often under, traditional software-based security solutions are less suitable. Hardware design is also increasingly driven by sustainability, with the need for reduced energy use and increased lifecycle for electronic solutions. Even more importantly, crypto research over the last few decades has demonstrated that HW platforms should be flexible, capable of implementing new algorithms without requiring a full redesign (Zhang et al., 2022).

To tackle these issues, this work seeks to:

- Implement a multi-hashing-based reconfigurable cryptographic engine
- Design a controller that can use a finite state machine to observe the system load at the time and handle the algorithm selection and the power consumption on the fly.
- Characterise the system performance and scalability on the Zynq-7000 FPGA platform using conventional cryptographic certifications and energy measurement standards.

These goals are achieved by proposing a reconfigurable, low-power system ready for future secure edge computing applications.

4. System architecture

The suggested architecture (Figure 1) adopts a modular structure where each cryptographic hash function, specifically SHA-2, SHA-3, SHAKE, and BLAKE2, is implemented as an independent processing core. A common control and data management unit interconnects these cores and coordinates their operation, ensuring efficient system performance and resource utilisation. The design specifically implements a finite-state machine (FSM) based adaptive control mechanism. This controller monitors various system metrics in real time, including processing load, thermal conditions, and quality-of-service requirements. With these inputs, the system dynamically selects the optimal hashing algorithm and adapts its operation mode between performance- and energy-oriented modes. Multiple optimisation techniques have been applied to improve efficiency and flexibility.

- Partial reconfiguration: Allows changing from one cryptographic core to another with no full system reset, which allows a more responsive and flexible implementation.
- Clock gating, which means it saves the dynamic power consumption by shutting off the clock signal going to inactive components.
- Optimised data path design – meets a low latency goal while efficiently using logic resources & maintains accuracy in computations.

The Vivado 2024.2.2 was used to develop and synthesise the system. Simulation-based analysis was used for functional validation and timing verification.

The common input-output interface of all hashing modules enables a seamless transition between operational modes. Also, to avoid hardware replication, most modules, such as padding and message scheduling, are common across all cores. To facilitate data transfer between the FPGA logic and the external processing interface, a dual-port memory architecture is used.

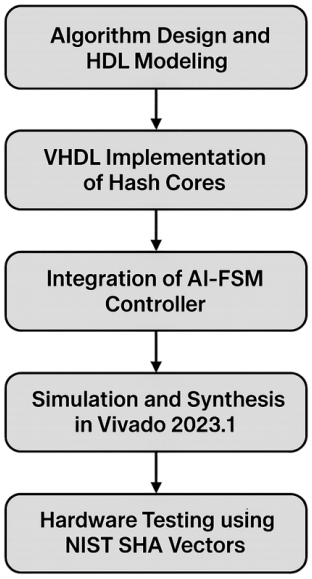

Figure 1: System architecture of the proposed multi-hash cryptographic engine

5. Methodology

A well-defined hardware design and analysis approach is adopted to develop the proposed cryptographic engine, thereby avoiding unnecessary efforts later to achieve functional correctness and energy-efficient performance. It starts with architectural modelling of the proposed multi-hash system, where each cryptographic algorithm is implemented as a separate hardware component. These VHDL-based modules are individually verified for functional correctness before integration at the system level. It is implemented on the Zynq-7000 FPGA using the Vivado 2024.2.2 design environment. This section describes the design flow followed, which includes synthesis, implementation, and timing analysis to ensure that all modules satisfy performance and resource requirements. Standard test benches, along with test vectors defined by the National Institute of Standards and Technology (NIST), are used for functional validation via simulation to confirm compliance with cryptographic standards.

The FSM is built as the central control unit for dynamic adaptability. This controller checks system parameters such as processing load and operating conditions and selects the appropriate hashing algorithm as needed. Based on real-time requirements, the FSM also controls the power-aware feature by turning specific modules on or off.

Energy efficiency is measured using power analysis tools built into the design environment. The trade-off between throughput and power consumption is characterised across various operating modes, including high-performance and low-power configurations. Clock gating and partial reconfiguration are explored and evaluated to assess their effectiveness in minimising dynamic power consumption. Performance evaluation includes throughput, latency, and resource utilisation. Throughput is defined based on processed data per unit of time, while latency is measured across various operational modes. Design scalability is evaluated based on resource usage, including logic elements and memory blocks. This methodology ensures that the evaluation of the proposed system focuses solely on functionality, performance, adaptability, and energy efficiency within a single experimental framework.

6. Results and evaluation

The proposed cryptographic engine was implemented on the Zynq-7020 FPGA and validated using standard test vectors defined by NIST for SHA-based algorithms. The evaluation focuses on key performance indicators, including throughput, power consumption, energy efficiency, and system adaptability under varying workload conditions. The experimental results (Table 1) demonstrate that the system achieves a maximum throughput of up to 1.25 Gbps in high-performance mode. Power consumption remains below 1 W across all operating conditions, confirming the suitability of the design for energy-constrained environments. The measured energy efficiency exceeds 1.2 Gbps/W, indicating a strong balance between performance and power usage.

Table 1: Performance summary of the proposed cryptographic engine

Metric	Value
Maximum Throughput	1.25 Gbps
Power Consumption	< 1 W
Energy Efficiency	| > 1.2 Gbps/W
Reconfiguration Time	< 20 µs
Energy Saving	35 % – 40 %

The reconfiguration mechanism enables switching between hashing algorithms with a latency below 20 µs, allowing the system to respond efficiently to dynamic operational requirements. Under varying workloads, including transitions between data-intensive processing and secure communication tasks, the control mechanism maintains stable and responsive system behaviour.

Comparative evaluation (Table 2, Figure 2) shows that the proposed architecture provides significant advantages over conventional FPGA-based single-algorithm implementations. In particular, energy consumption is reduced by approximately 35 % to 40 % compared to fixed-function SHA-3 accelerators. Furthermore, when compared with software-based implementations running on embedded processors, the proposed hardware design achieves up to fifteen times higher throughput, along with reduced processing latency.

Table 2: Comparison with existing implementations

Implementation Type	Throughput	Power (W)	Energy Efficiency (Gbps/W)	Flexibility
Proposed Work	1.25 Gbps	< 1	> 1.2	High (multi-hash)
FPGA-SHA-3 (Fixed)	~1.0 Gbps	~1.2	~0.8	Low
FPGA Lightweight Design	~0.6 Gbps	~0.7	~0.85	Medium
Software (Cortex-A9)	~0.08 Gbps	> 1.5	Very Low	High

These results confirm that the proposed system provides an effective and scalable solution for secure and energy-efficient edge computing applications.

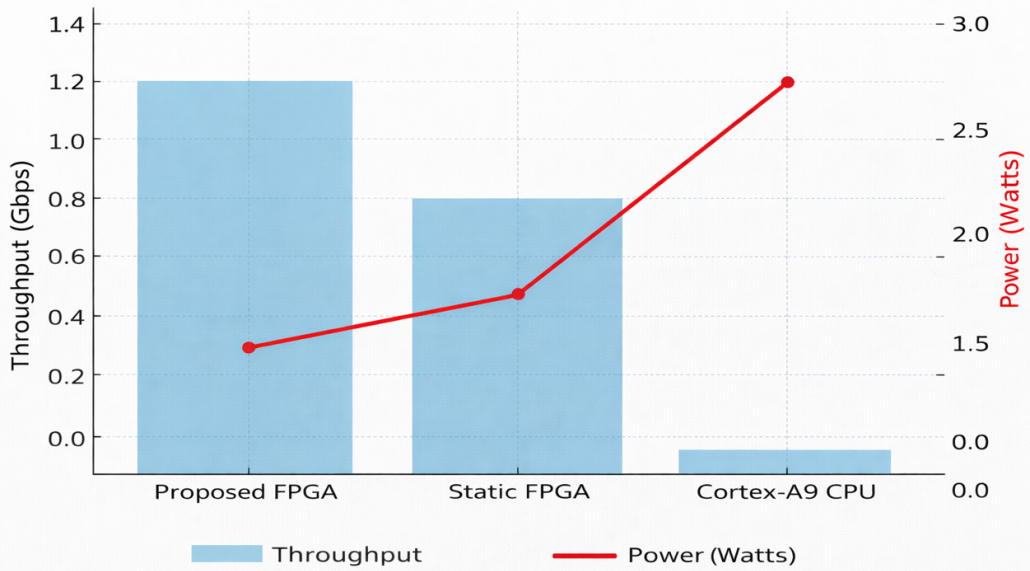

Figure 2: Throughput and power comparison of the proposed FPGA, static FPGA, and Cortex-A9 CPU

7. Relevance to conference themes

This work aligns well with the conference's key message on energy-efficient, reconfigurable hardware solutions. This architecture is partly reconfigurable, which extends the useful time period for an FPGA-based system and can lead to sustainability and reduced hardware waste.

Furthermore, it even enhances the security of data processing across applications, from healthcare and education to smart services, which are increasingly relevant to younger demographics who are heavily reliant on digital technologies.

Moreover, the design incorporates modern research practices, sophisticated development tools, and adaptable hardware concepts to facilitate innovative, streamlined engineering practices.

8. Conclusions

This work presents a reconfigurable multi-algorithm cryptographic engine designed to support secure and energy-efficient edge computing applications. The implementation on the Zynq FPGA platform demonstrates a balanced trade-off between performance, adaptability, and power consumption, making it suitable for deployment in resource-constrained environments.

The ability to dynamically select hashing algorithms at runtime enhances system flexibility and allows the architecture to respond effectively to varying application requirements. Experimental results confirm that the proposed design achieves high throughput while maintaining low power consumption, highlighting its potential as a scalable and sustainable solution for modern embedded systems.

References

- Dolmeta A., Martina M., Masera G., 2023, Comparative Study of Keccak SHA-3 Implementations. Cryptography, 7(4), 60, https://doi.org/10.3390/cryptography7040060.
- El Moumni S., Fettach M., Tragha A., 2019, High throughput implementation of SHA-3 hash algorithm on FPGA. Microelectronics Journal, 93, 104615, https://doi.org/10.1016/j.mejo.2019.104615.
- Kahri F., Mestiri H., Bouallegue B., Machhout M., 2016, High Speed FPGA Implementation of Cryptographic KECCAK Hash Function. Journal of Circuits, Systems and Computers, 25(4), 1650026, https://doi.org/10.1142/S0218126616500262.
- National Institute of Standards and Technology (NIST), 2015, FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, http://dx.doi.org/10.6028/NIST.FIPS.202.
- Sideris A., Sanida T., Dasygenis M., 2020, High Throughput Implementation of the Keccak Hash Function Using the Nios-II Processor. Technologies, 8(1), 15, https://doi.org/10.3390/technologies8010015.
- Xiong S., Liu D., Lu J., Li A., Huang T., Yang C., Hu A., Zhang Y., 2024, A Lightweight Folded Keccak-Based SHA-3 for Resource-Constrained Embedded Security, in: 2024 IEEE 17th International Symposium on Embedded Multicore/Many-Core Systems-on-Chip (MCSoC), Kuala Lumpur, Malaysia, 194–201, https://doi.org/10.1109/MCSoC64144.2024.00041.
- Zhang X., Liu B., Zhao Y., Hu X., Shen Z., Zheng Z., Liu Z., Chong K.-S., Yu G., Wang C., Zou X., 2022, Design and Analysis of Area and Energy Efficient Reconfigurable Cryptographic Accelerator for Securing IoT Devices. Sensors, 22, 9160, https://doi.org/10.3390/s22239160.