IMPLEMENTATION OF A LIGHTWEIGHT CHACHA20 ENCRPTION - DECRYPTION CORE ON SPARTAN-7 FPGA

Project Reference No.: 49S_BE_3072

College : Rajarajeswari College of Engineering, Bengaluru
Branch : Department of Electronics and Communication Engineering
Guide(s) : Dr. Sunitha R
Student(s) : Ms. Preethu J M
Ms. Raksha M
Mr. Rohith S
Ms. Vaishnavi H M

Keywords:

ChaCha20, Stream Cipher, FPGA Implementation, Hardware Acceleration, Double-Round Function, Cryptography, High Throughput, Low Resource Utilization, Embedded Systems, Real-Time Encryption, Digital Logic Design, Parallel Processing.

Introduction:

In today's digitally connected world, the need for fast, secure, and energy-efficient cryptographic solutions is crucial, especially in embedded systems like IoT devices, wireless sensor networks, medical electronics, and defense applications, where power, latency, and computational resources are limited. ChaCha20, standardized in RFC 8439, is widely adopted due to its lightweight design, strong security, and efficient performance using simple operations such as modular addition, XOR, and bit rotation, which also reduce vulnerability to timing attacks. However, software implementation on general-purpose processors can still limit performance in high-speed, low-power systems. To address this, the project implements the ChaCha20 stream cipher in hardware using Verilog HDL on an FPGA platform, enabling lower latency, higher throughput, reduced CPU load, and improved resistance to side-channel attacks. The design integrates modules like Key Expansion, QuarterRound, DoubleRound, and XOR into a compact pipeline and includes a VIO-based interface in Xilinx Vivado for easy control and monitoring, resulting in a scalable and efficient cryptographic solution for modern embedded applications.

Objectives:

1. To design and implement the ChaCha20 stream cipher using Verilog HDL at the RTL level.
2. To develop an efficient encryption–decryption system suitable for FPGA-based embedded applications.
3. To verify the functionality of the design through simulation and hardware testing on FPGA.
4. To evaluate the performance in terms of speed, power consumption, and resource utilization.

Methodology:

The project proposed work involves the design and implementation of the ChaCha20 stream cipher using Verilog HDL at the Register Transfer Level (RTL). Initially, the algorithm was analyzed to understand its state matrix structure, ARX operations, and round transformations. The design was then modeled into modular components such as key expansion, round processing, and XOR-based encryption using a synchronous, clock-driven approach with FSM control. Functional verification was carried out using a testbench to ensure correct encryption and decryption. The verified design was synthesized and implemented on a Xilinx Spartan-7 FPGA using Vivado, followed by placement, routing, and bitstream generation. Hardware validation was performed using the Virtual Input/Output (VIO) IP core for real-time monitoring. Finally, performance evaluation was conducted based on operating frequency and power consumption to assess suitability for embedded and low-power applications.

Result and Conclusion:

In conclusion, the project demonstrates an efficient RTL-based hardware implementation of the ChaCha20 stream cipher, achieving reliable encryption and decryption on an FPGA platform. The use of simple ARX operations enables a lightweight and timing-safe design suitable for embedded and IoT systems. The successful verification through simulation and hardware testing validates the feasibility of FPGA-based cryptographic acceleration. This work provides a strong foundation for further enhancements such as authenticated encryption and performance optimization for real-world secure communication systems.

Design	Power (W)
Existing Work	0.202
Proposed ChaCha20 Design	0.046

Figure 1: COMPARISON OF POWER WITH BASE PAPER

References:

- W. Grignani, K. G. Q. Santana, D. A. Santos, L. Dilillot, and D. R. Melo, ”Implementation and reliability evaluation of a ChaCha20 stream cipher hardware accelerator,” in 2024 IEEE Intl. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFT), 2024, pp. 1-6
- Z. Wang, H. Chen, and W. Cai, ”A hybrid CPU/GPU scheme for optimizing ChaCha20 stream cipher,” in Proc. IEEE Intl. Conf. Parallel Distributed Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw. (ISPA/BDCloud/SocialCom/SustainCom), 2021, pp. 101–106
- N. At, J.-L. Beuchat, E. Okamoto, I. San, and T. Yamazaki, ”Compact hardware implementations of ChaCha, BLAKE, Threefish, and Skein on FPGA,” in Proceedings of the 2013 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2013, pp. 1-6
- O. Esuruoso, ”High speed FPGA implementation of cryptographic hash function,” M.S. thesis, Univ. Windsor, Windsor, ON, Canada, 2011.

Future Scope:

The future scope of this project includes:

1. Integration of Poly1305 authentication to extend the design into a complete authenticated encryption system (ChaCha20-Poly1305).
2. Implementation of pipelining and parallel processing techniques to improve throughput and overall performance.
3. Enhancement of security and reliability by incorporating side-channel attack resistance and fault-tolerance mechanisms.