IEEE-iSES 2025 Special Session

High-Speed Hardware Accelerator for Cryptographic functions

Scope

Secure communication is necessary to protect data privacy and prevent unauthorized access, theft, and modification of sensitive information by using methods like encryption, authentication, and integrity checks. It safeguards personal details, business secrets, and, ensuring confidentiality, accuracy, and trustworthiness in online interactions and building confidence in digital systems against growing cyber threats.

We use different kind of algorithms for confidentiality/integrity/authentication such as Block cipher (e.g 3DES, DES, AES), Stream cipher (RC4), public Key (RSA, ECC) and MACs/HMAC based on MD5, SHA etc

Hardware implementations of cryptographic algorithms are needed to provide high speed, increased security, and improved power efficiency compared to software implementations.

Example : SSL, IPsec protocol provides security, integrity and authentication at transport and Network layer

- AES/DES/3DES is typically used securing data traffic, RSA (public key cryptography) is used for sharing symmetric key to other party and HMAC is used for data integrity.

Task:

Design and implement a hardware accelerator for the following cryptographic algorithm which optimizes for high throughput, low latency, and energy efficiency. The solution should be suitable for integration into an ASIC or FPGA.

- AES-128 bit
- RSA-2048 bit
- HMAC based on MD5 or SHA-1

Requirements

- **Supported Algorithm:** AES-128, RSA-2048, HMAC (MD5).
- **High-Speed Architecture:**

    - Propose and implement architectural optimizations (e.g. High speed adder, multipliers, pipelining, parallelism, resource sharing).
    - Support for high data rates & Low latency
- **Power and Area Efficiency:**
    - Analyze and optimize power consumption and silicon area.
- **Verification:**
    - Functional verification using test vectors for encryption & decryption
    - Performance benchmarking (throughput, latency, power).
- **Deliverables:**
    - RTL design (Verilog/VHDL/SystemVerilog)
    - Target platform – FPGA (Altera or Xilinx) or ASIC (Synopsys/Cadence etc)
    - Technical report detailing architecture, optimizations, results, and trade-offs.
    - Live demo or simulation or FPGA prototype.

Evaluation Criteria

- **Correctness** – Implementation should adhere to standard protocol. Show few working standard vectors in the demo/simulation
- **Throughput -** Throughput refers how much data can be processed in a sec (for e.g a throughput of 1Gbps means 1Giga bit of data can be processed in a second)
- **Latency – (for e.g** How many cycles consumed in result generation for AES operation)
- **Max frequency** - List max frequency of operation
- **Power and Area Efficiency**
- **Design Innovation**
- **Quality of Documentation and Presentation**

Session Organizers

- Surendra Tadi, Qualcomm India Pvt Ltd, surendratadi@gmail.com
- Mayank Parasrampuria, Google India Pvt Ltd, mayankp406@gmail.com

Topics/ Keywords

- Hardware Assisted Security, Security by Design

Important Dates:
Launch: 14 October, 2025
Last date to receive application: 30 October, 2025
Orientation session: 3 November, 2025,
Last day of implemented idea submission: 30 November, 2025

Submission accepted through Microosft CMT:
https://cmt3.research.microsoft.com/User/Login?ReturnUrl=%2FIEEEiSeS2025

The applicant has to submit the application under Design Contest- HW accelerators for Cryptographic functions.