Optimizing TLS Cryptographic Operations on RISC-V SoC with OpenTitan RoT

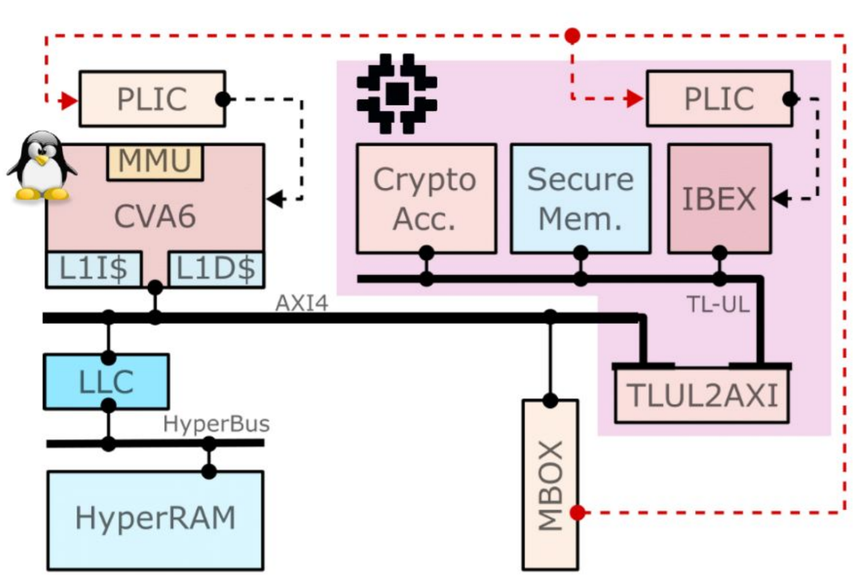
A. Musa[1], E. Parisi[2], L. Barbierato[3], E. Patti[3], A. Bartolini[1], A. Acquaviva[1], F. Barchi[1]

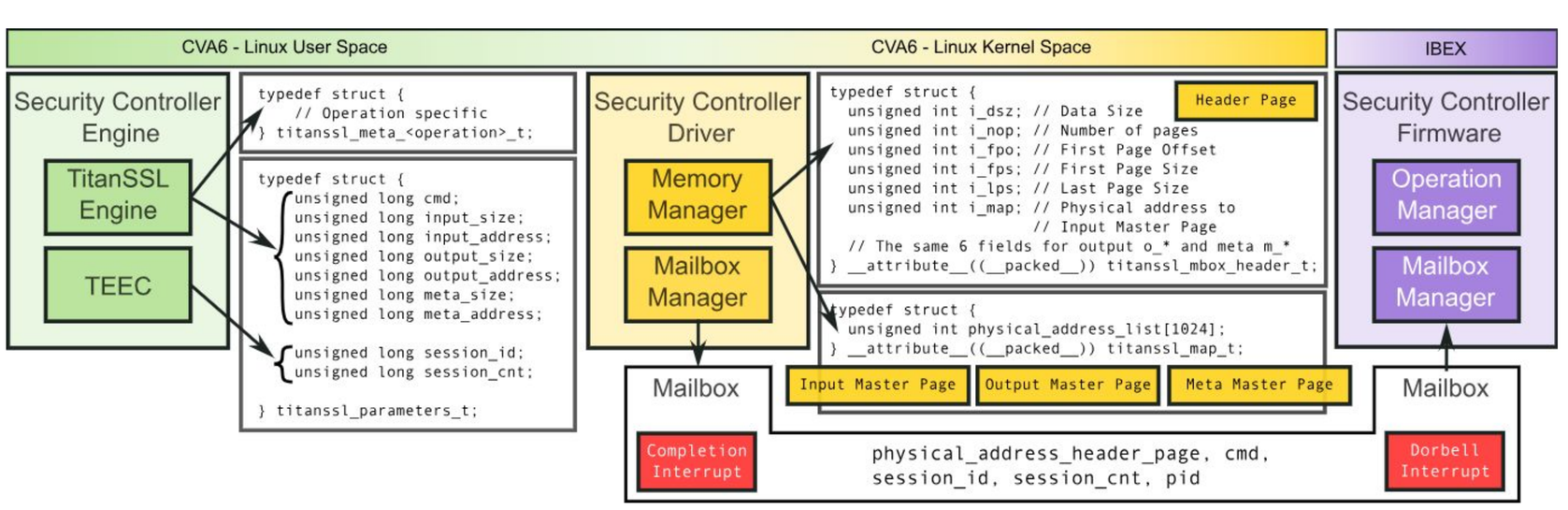
[1]*Department of Electrical, Electronic, and Information Engineering (DEI) – University of Bologna, Italy*

[2]*Barcelona Supercomputing Center - Barcelona, Spain*

[3]*Department of Control and Computer Engineering (DAUIN) – Polytechnic of Turin, Italy*

<alberto.musa@unibo.it>





1. Motivation and Contribution

Secure communication is essential in embedded systems, particularly in resource-constrained environments. This work integrates **OpenTitan**, a hardware **Root-of-Trust** (RoT), within a RISC-V-based SoC to accelerate cryptographic operations for **Transport Layer Security** (TLS). The key contributions include:

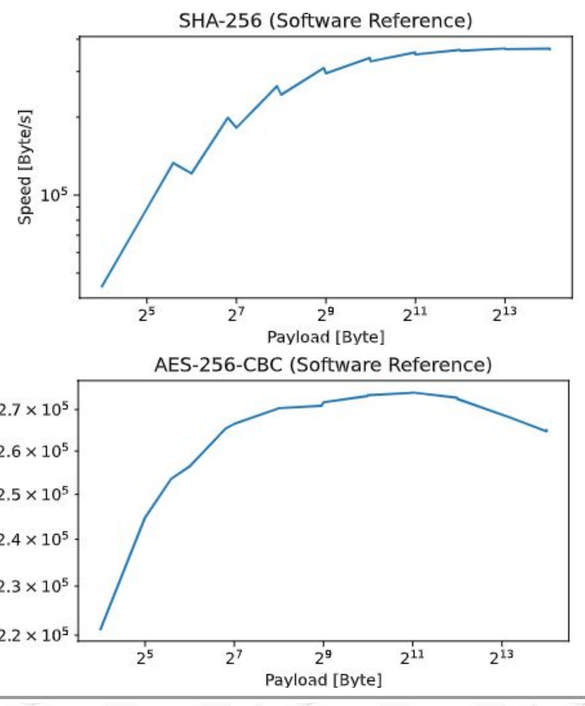
- **Development of TitanSSL**, a cryptographic software stack leveraging OpenTitan's hardware accelerators for cryptographic tasks.
- **Offloading of AES, SHA, and RSA operations** to dedicated hardware accelerators. Comprehensive performance evaluation of TitanSSL's highlights the balance between computational overhead and acceleration benefits.
- **Providing a secure backend for OpenSSL** within the SoC architecture and integrating OpenSSL to support the **TLS_RSA_WITH_AES_256_CBC_SHA256** cipher suite.

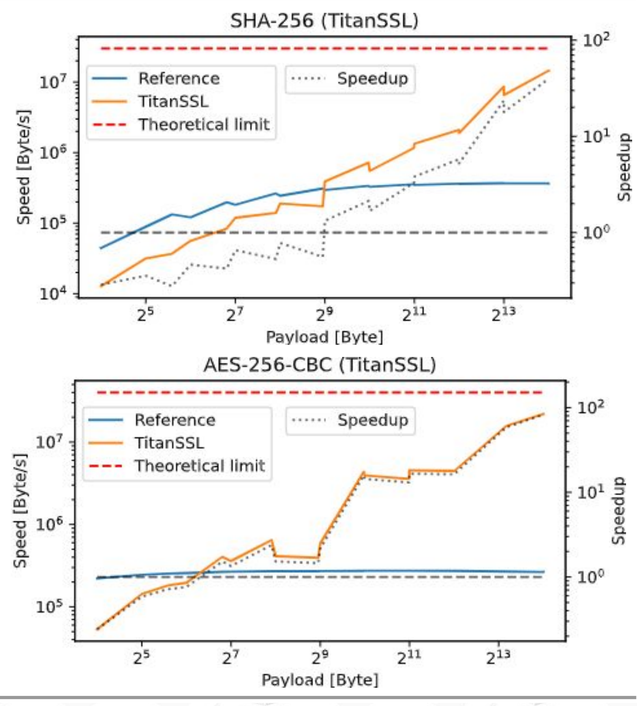
2. System Architecture and Implementation

The system consists of a **CVA6** application processor running Linux, an OpenTitan-based security subsystem, and a communication mechanism via a mailbox interface. OpenSSL functions are extended through an **OpenSSL Engine** and a **Linux driver** to delegate cryptographic operations to OpenTitan. The firmware on OpenTitan directly interfaces with hardware accelerators, ensuring secure execution. A custom **communication protocol** was designed to efficiently handle data exchange between the CVA6 and OpenTitan, addressing challenges like synchronization and latency. Shared **HyperRAM** is used for data transfer, with address translation and locking mechanisms ensuring secure access. Key challenges include:

- Lack of MMU in OpenTitan, requiring manual address management.
- Cache asymmetry between CVA6 and OpenTitan, requiring efficient data synchronization.

Payload	SHA [KiB/s]		Speedup	OT	AES [KiB/s]		Speedup	OT
[Byte]	OpenSSL	TitanSSL		Limit	OpenSSL	TitanSSL		Limit
16	43	12	0.29x	0.0 %	216	52	0.24x	0.1 %
32	87	31	0.36x	0.1 %	239	140	0.59x	0.4 %
48	130	36	0.28x	0.1 %	248	177	0.72x	0.5 %
64	118	55	0.46x	0.2 %	250	191	0.76x	0.5 %
112	194	82	0.42x	0.3 %	259	394	1.52x	1.0 %
128	178	116	0.65x	0.4 %	260	350	1.35x	0.9 %
240	257	137	0.53x	0.5 %	264	627	2.38x	1.6 %
256	238	186	0.78x	0.6 %	264	402	1.52x	1.0 %
496	303	169	0.56x	0.6 %	265	386	1.46x	1.0 %
512	288	382	1.33x	1.3 %	265	578	2.18x	1.5 %
1008	330	705	2.13x	2.4 %	267	4233	15.86x	10.8 %
1024	320	537	1.68x	1.8 %	267	3840	14.38x	9.8 %
2032	347	1136	3.27x	3.9 %	268	3501	13.08x	9.0 %
2048	341	1300	3.82x	4.4 %	268	4436	16.57x	11.4 %
4080	355	2049	5.78x	7.0 %	267	4352	16.33x	11.1 %
4096	352	1850	5.25x	6.3 %	266	4338	16.30x	11.1 %
16384	357	14222	39.80x	48.5 %	259	21333	82.45x	54.6 %





3. Summary of Findings

Benchmarking on an **FPGA** prototype demonstrates substantial improvements in performance, highlighting the efficiency of the hardware-accelerated solution.

- Significant speedup of **82x for AES-256-CBC** (tested with a 16KiB payload), **39x for SHA-256** (tested with a 16KiB packet digest), and **1.8x for RSA 1024 Encryption**.
- The OpenTitan solution reaches about **50% of the hardware accelerator's maximum performance** due to memory inefficiencies and cycle overhead during cryptographic tasks.

These results demonstrate that offloading cryptographic operations to OpenTitan enhances both security and performance, making it a viable solution for secure embedded systems. Future work will focus on extending support to additional TLS cipher suites and improving performance.

RISC-V SUMMIT EUROPE 2025

12 - 15 May 2025
La Cité des Sciences et de l'Industrie, Paris

[1] Maicol Ciani et al. "Cyber Security aboard Micro Aerial Vehicles: An OpenTitan-based Visual Communication Use Case". In: 2023 IEEE ISCAS. 2023.
[2] F. Zaruba et al. "The Cost of Application-Class Processing: Energy and Performance Analysis of a Linux-Ready 1.7-GHz 64-Bit RISC-V Core in 22-nm FDSOI Technology". In: IEEE VLSI (2019)
[3] lowRISC CIC. OpenTitan Official Documentation. https://opentitan.org/book/doc/introduction.html. 2019.
[4] Alberto Musa et al. "TitanSSL: Towards Accelerating OpenSSL in a Full RISC-V Architecture Using OpenTitan Root-of-Trust". In: SafeComp 2024, pp. 169–183.