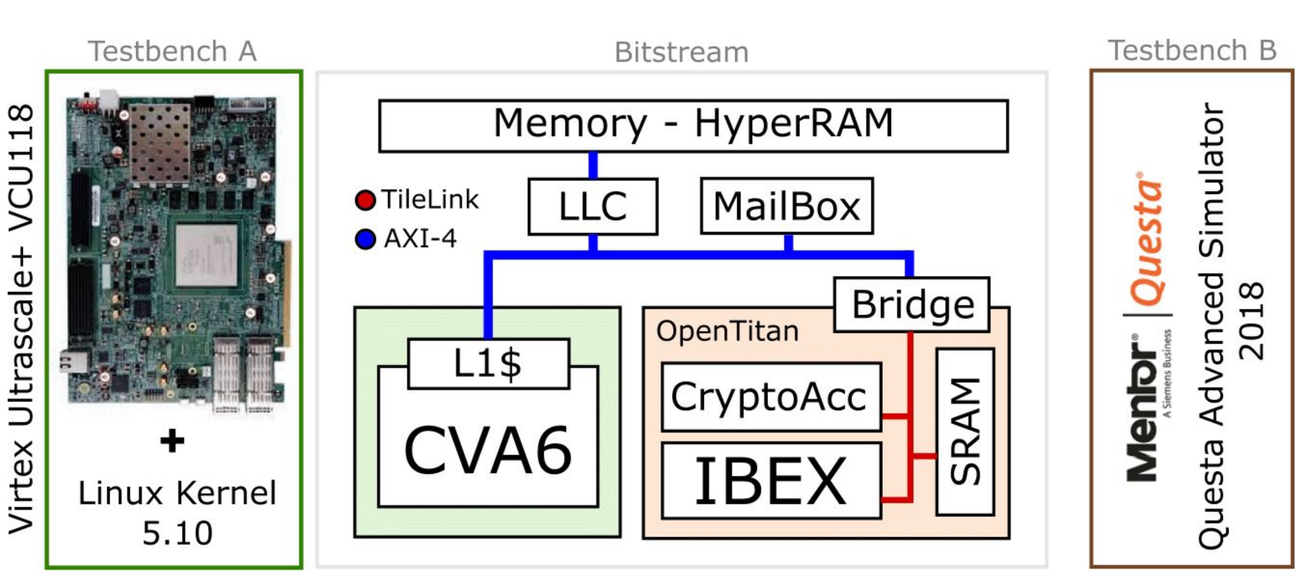
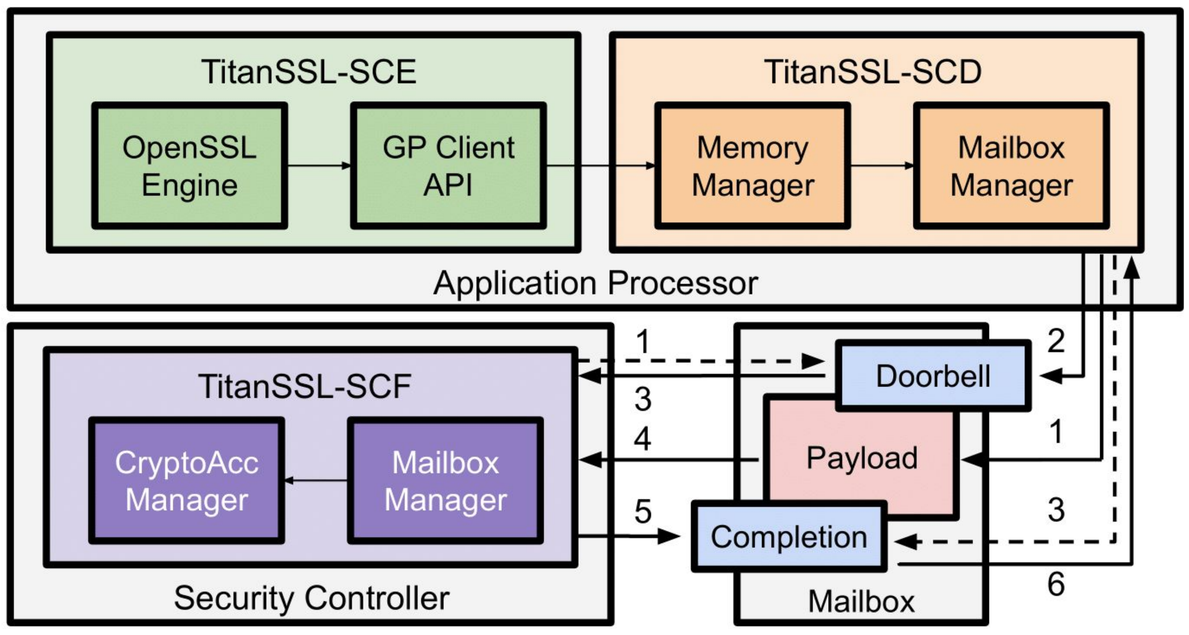
TitanSSL: Towards Accelerating OpenSSL in a Full RISC-V Architecture Using OpenTitan

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

[1]*Department of Electrical, Electronic, and Information Engineering (DEI) – University of Bologna, Italy*
[2]*Department of Control and Computer Engineering (DAUIN) – Polytechnic of Turin, Italy*

alberto.musa@unibo.it





Motivation and Contribution

- The rapid evolution of **cyber-physical systems** (CPS) demands robust security measures. Utilizing **OpenTitan** in **open-hardware System-on-Chip** (SoC) technology *offers a promising avenue for enhancing security, especially in accelerating cryptographic operations*.
- Introduction of **TitanSSL**, *a software stack leveraging OpenTitan's hardware accelerators for cryptographic tasks*. This addresses the challenge of providing *a secure backend for OpenSSL within the SoC architecture*. Additionally, *comprehensive evaluation of TitanSSL's performance* reveals insights into the trade-offs between computational overhead and speed-up.

Security Implications & Assumptions

- Integration of **OpenTitan** as a ***Root-of-Trust*** enhances the overall security posture of the SoC, e*nsuring secure boot and isolation of critical operations.* Leveraging hardware accelerators for cryptographic tasks improves *resistance against side-channel attacks and enhances system resilience*. TitanSSL orchestrates *secure communication between the application processor and the security controller, mitigating potential vulnerabilities in cryptographic operations*.
- Assumptions include *the integrity and reliability of OpenTitan's hardware components*, proper implementation and configuration of TitanSSL components for *secure communication and key management, and trust in the underlying firmware and software stack*, **including OpenSSL**, for handling cryptographic requests securely.

Table 1: *TitanSSL results in terms of cycles per byte.*

Test	Cycles per Byte			Speedup	Overhead
	OpenSSL	TitanSSL	SCF		
sha					
16 B	462	877	61	0.5	93.1 %
64 B	216	231	27	0.9	88.2 %
256 B	127	71	20	1.8	72.1 %
1024 B	104	31	18	3.4	41.6 %
aes					
16 B	155	947	136	0.2	85.6 %
64 B	145	270	67	0.5	75.2 %
256 B	142	101	51	1.4	50.1 %
1024 B	141	60	47	2.4	21.2 %
rsa-public					
512 b	2 430	2 678	2 396	0.9	10.5 %
1024 b	3 815	2 250	2 109	1.7	6.3 %
2048 b	5 126	2 790	2 720	1.8	2.5 %
rsa-private					
512 b	30 518	8 618	8 337	3.5	3.3 %
1024 b	68 531	23 016	22 875	3.0	0.6 %
2048 b	193 955	78 140	78 070	2.5	0.1 %

Summary of Findings

- Significant speed-ups observed in cryptographic operations, with **SHA-256 and AES-256-CBC** exhibiting enhancements of **3.4x** and **2.4x,** respectively. **RSA** operations also demonstrated improvements, achieving speed-ups of approximately **1.8x** and **3.5x**.
- Despite overhead, TitanSSL efficiently utilizes OpenTitan's hardware accelerators, showcasing its effectiveness in accelerating cryptographic workloads while securely operating within OpenTitan's environment and leveraging its root-of-trust capabilities

[1] Bryan Parno et al. “Roots of Trust”. In: Bootstrapping Trust in Modern Computers. New York, NY: Springer New York, 2011, pp. 35–40.
[2] Maicol Ciani et al. “Cyber Security aboard Micro Aerial Vehicles: An OpenTitan-based Visual Communication Use Case”. In: 2023 IEEE ISCAS. 2023.
[3] 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)
[4] lowRISC CIC. OpenTitan Official Documentation. https://opentitan.org/book/doc/introduction.html. 2019.
[5] Pasquale Davide Schiavone et al. “Slow and steady wins the race? A comparison of ultra-low-power RISC-V cores for Internet-of-Things applications”. In: PATMOS. 2017.
[6] Scott Johnson et al. “Titan: enabling a transparent silicon root of trust for cloud”. In: Hot Chips: A Symposium on High Performance Chips. Vol. 194. 2018. 2 RISC-V Summit Europe, Munich.

RISC-V SUMMIT EU JUNE 24 – 28 | MUNICH 2024