

7th INTERNATIONAL CONFERENCE ON PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2026)

SEPTEMBER 10-11th, 2026

**BHARAT-TPM: Design and ASIC Implementation of an SPI Based AXI
Enabled RNG Accelerator**

Mahima Agarwal, Soumya G, Dr. Raja Sekar K, Aneesh Raveendran, Vivian D, Hari
Babu P, Dr. S D Sudarsan

Centre for Development of Advanced Computing (C-DAC), Bangalore

INTRODUCTION & MOTIVATION

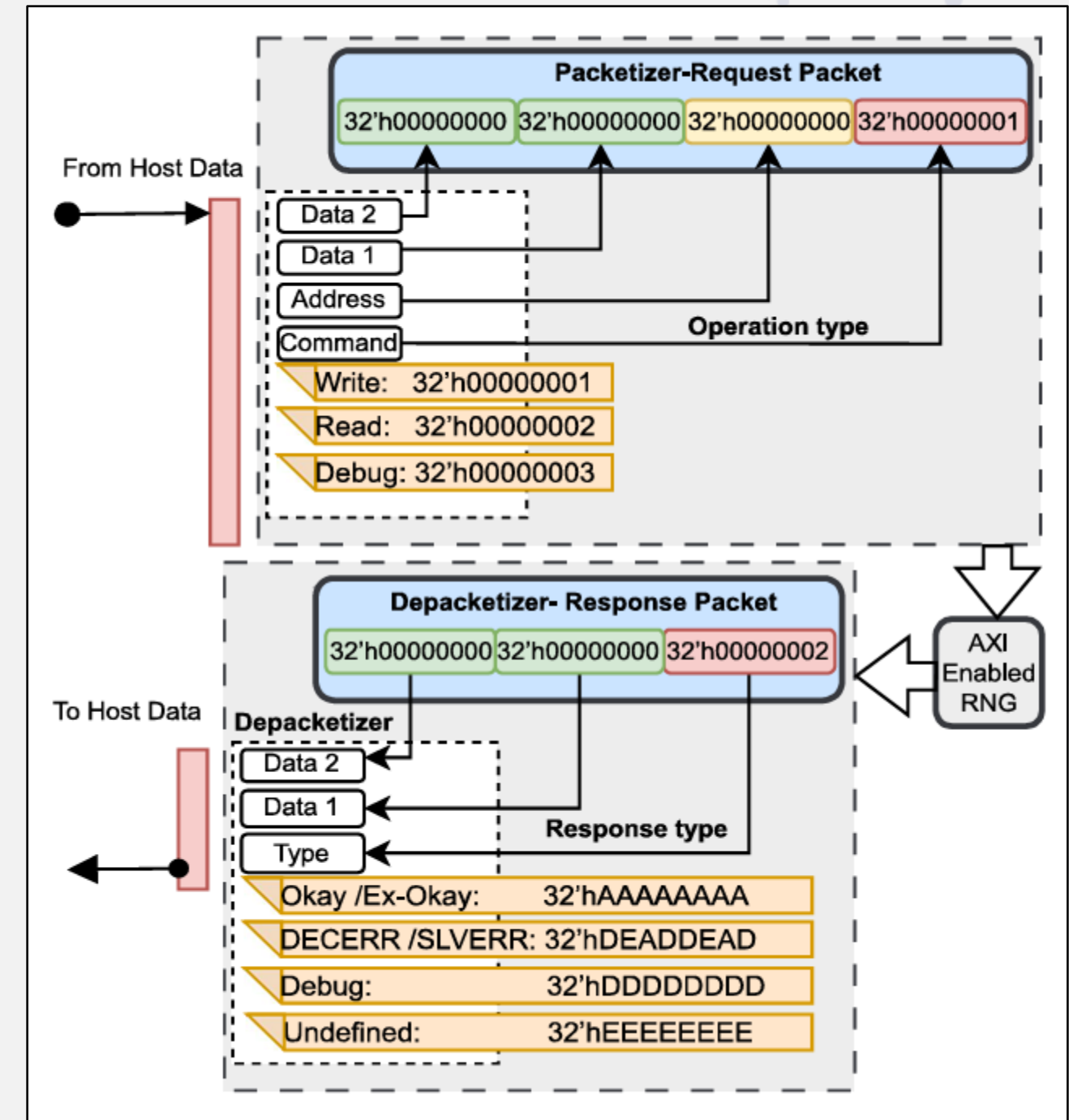
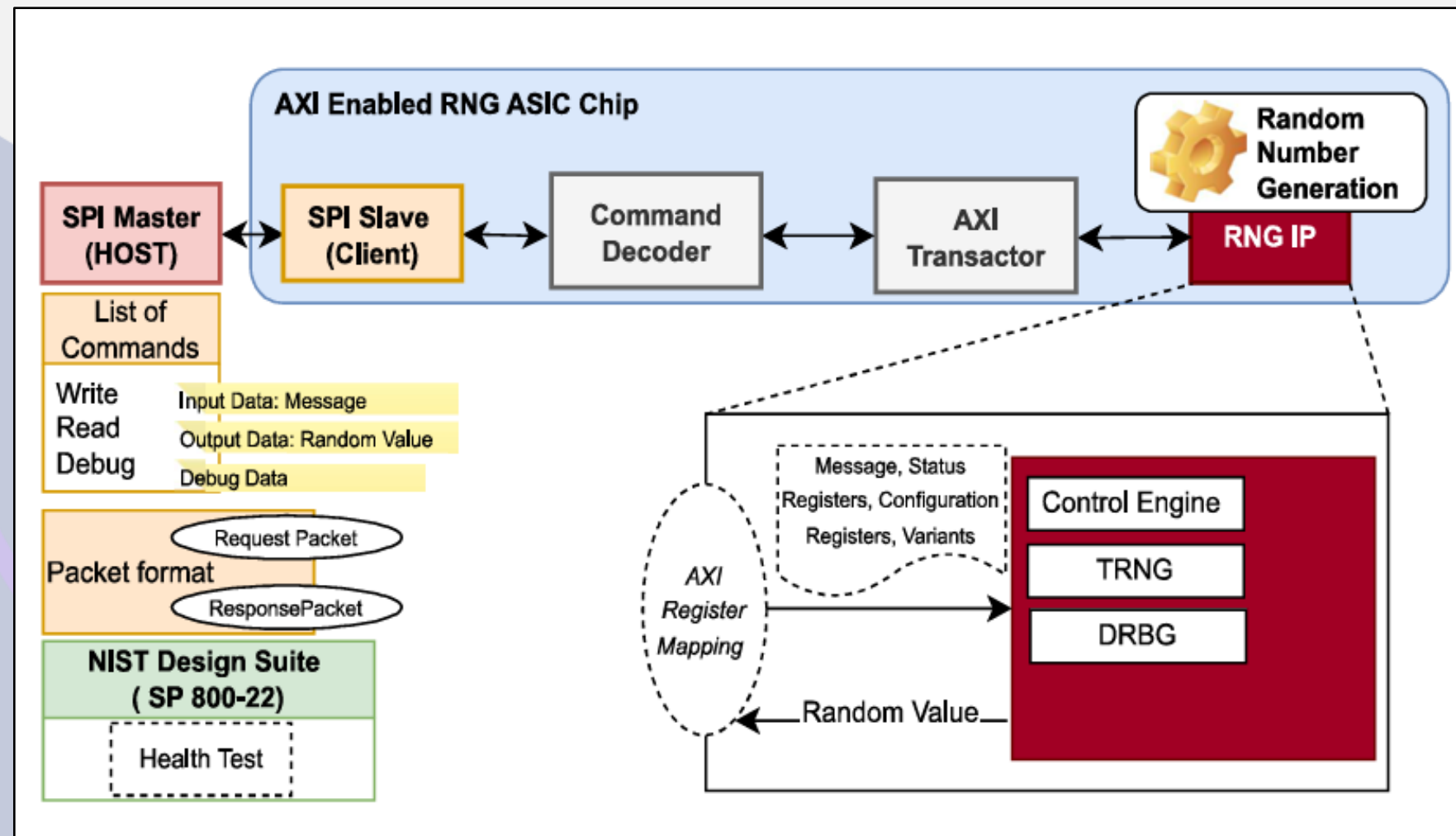
- TPM based secure platforms require high quality entropy for cryptographic operations.
- Hardware RNGs are essential for secure key generation and PKI applications.
- AXI enabled RNG accelerators require standalone validation before SoC integration.
- Existing designs emphasize throughput and processor integration, with limited support for external SPI based validation.
- A reusable, packet based SPI to AXI validation architecture for standalone validation of AXI-based cryptographic IP cores.

PROBLEM STATEMENT & OBJECTIVES

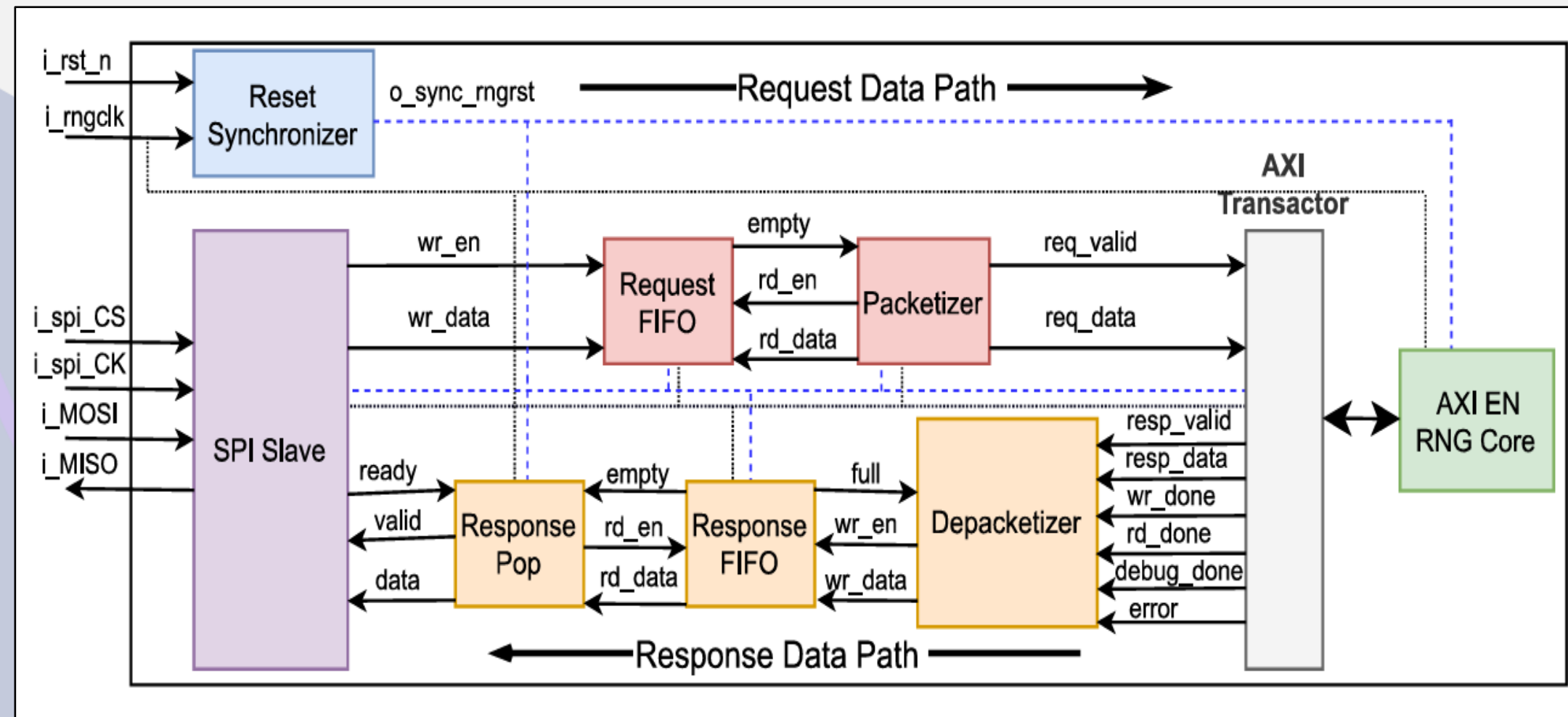
Existing RNG accelerator implementations do not address standalone validation of AXI based cryptographic accelerators and SPI interfaces before integration into a RISC-V based TPM SoC.

- **Develop:** SPI-based external validation interface
- **Integrate:** Packet-based SPI-to-AXI architecture
- **Generate:** TRNG + DRBG random numbers
- **Verify:** NIST SP 800-90B & SP 800-22 validation
- **Implement:** VCU108 FPGA prototype + SCL 180 nm ASIC synthesis

PROPOSED METHODOLOGY



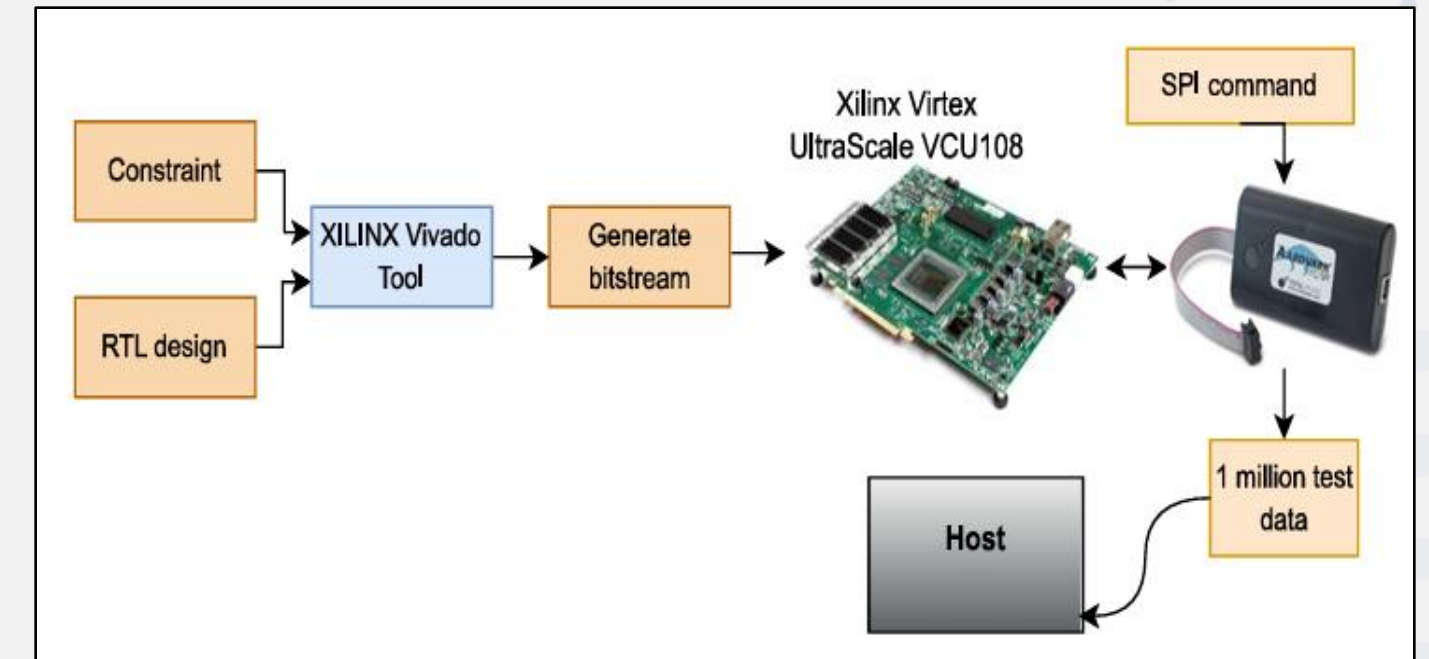
ARCHITECTURE / DESIGN DETAILS



- SPI enabled AXI based RNG accelerator with packet based communication.
- 128-bit request and 96-bit response packet formats.
- Supports generation of random data and status information.
- Request data are packetized, buffered, and transferred through the AXI interface for RNG processing.

EXPERIMENTAL SETUP / IMPLEMENTATION

Parameter	Details
RTL Design	Verilog/ System Verilog
Implementation Flow	RTL → ASIC Check → Simulation → FPGA Prototype → ASIC Synthesis
Tool Used	Cadence SimVision/ JasperGold/ Genus/ Vivado
Cryptographic Test Vectors	SP800-90A/C
Functional Test Cases	240



RESULTS & COMPARATIVE ANALYSIS

Successfully validated the RNG accelerator through standalone SPI based verification, AXI integration, FPGA prototyping, and 180 nm ASIC synthesis.

29,769 Sequential Cells

3.708 mm² Cell Area

90,797 Combinational Cells

Design	Platform	LUT	FF	Entropy Rate	Frequency (MHz)	Throughput (Mbps)
[23] (TRNG)	Cyclone IV	-	-	0.981	13	52
[24] (TRNG)	Kintex-7	15	8	0.990	550	550
[25] (TRNG)	Zynq	-	-	0.985	200	2
[26] (TRNG)	Virtex-6	-	1115	0.975	6.25	6.25
[27] (TRNG)	Kintex-7	30	30	0.995	400	2400
This work (TRNG+DRBG)	VCU108	21847	30069	0.995	250	37.74

CONCLUSION, FUTURE SCOPE & References

Conclusion

- Proposed a reusable hardware validation framework for AXI based cryptographic IPs.
- Developed a packet based SPI to AXI architecture for standalone validation.
- Implemented an AXI enabled RNG accelerator.
- Functionally verified using NIST Health Test.
- Validated on Xilinx VCU108 FPGA.
- Demonstrated ASIC synthesis using SCL 180nm technology.

Future Scope

- Integrate the validated RNG accelerator into BHARAT-TPM.
- Verify the accelerator using bare-metal application programs.
- Validate integrated TPM functionality using TCG TPM commands.
- Extend the validation framework to other cryptographic accelerators.

References:

- [1] Trusted Computing Group, *TPM 2.0 Library Specification*, 2024
- [2] Soumya G Hosmani et al., "BHARAT-TPM: Micro-Architecture Design of Scalable Hardware Random Number Generator for a RISC-V Trusted Platform Module," 2026 39th Int. Conf. on VLSI Design and 2023 25th Int. Conf. on Embedded Systems (VLSID), Jan 2026.
- [3] A. Rukhin et al. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (SP 800-22 Rev. 1a)*, NIST, 2010.

THANK YOU