Final Year Design Project Showcase
Batch-2022
Year 2026

Department: of Telecommunications Engineering Name of Programme: Telecommunications Engineering	
1	**Project Title:** AES-GCM and Kyber (Quantum Safe Encryption System) on a 32-bit Pipeline core RISC-V Processor
2	**Project Idea:** The rapid advancement of quantum computing threatens classical public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC), both of which remain vulnerable to Shor's algorithm and expose today's encrypted communications to "harvest-now, decrypt-later" attacks. This project proposes a hardware-based hybrid quantum-safe encryption system which pairs a HPS-based AES-256 Galois/Counter Mode (GCM) authenticated encryption SoC that delivers high speed, area efficiency, and high throughput based with CRYSTALS-Kyber-1024, a NIST-standardized lattice-based post-quantum Key Encapsulation Mechanism (KEM), both realized as custom, silicon-proven hardware accelerators built around a self-designed 32-bit, 5-stage pipelined RISC-V (RV32I) processor. The resulting system delivers proven symmetric-key throughput alongside quantum-resistant key exchange in a fully open, vendor-independent hardware stack suited to secure IoT, embedded, financial, and defense-grade communication infrastructure preparing for the global post-quantum migration.
3	**Process** The project followed a rigorous, six-phase, bottom-up development methodology that isolated and independently validated each subsystem before system-level integration: I. **Phase I Algorithmic Golden Model:** AES-128/192/256 was hand-implemented in Python without any cryptographic libraries including GF(2^8) arithmetic, the Rijndael S-Box, and the full key schedule producing a bit-accurate reference validated against NIST FIPS-197 and GCM test vectors. II. **Phase II RTL Design & Architectural Exploration:** The Python model was translated into synthesizable Verilog and iterated through seven distinct architectures non-pipelined, 3-stage pipelined (BRAM-accelerated), dual-core parallel, and area-optimized single-round FSM designs each independently verified through functional verification in ModelSim. III. **Phase III Hardware/Software Co-Design (SoC): I**n the final AES-GCM SoC (System on Chip) architecture, the computationally heavy Key Expansion runs as

	C code on the ARM Cortex-A9 Hard Processor System (HPS) of an Intel Cyclone V DE10 standard (5CSXFC6D6F31C6N) , streaming round keys to a custom AES-GCM IP core over an AXI-to-Avalon bridge built in Quartus Platform Designer. IV. **Phase IV Multi-Platform Hardware Validation:** designs were synthesized and tested with live UART/RealTerm data exchange on the Intel Cyclone V FPGA Starter Kit (5CGXFC5C6F27C7N) and DE10-Standard SoC board, and cross-verified on Xilinx Arty Z7 (XC7Z010CLG400-1) and PYNQ-Z1 (XC7Z020CLG400-1) boards. V. **Phase V Post-Quantum Cryptography:** CRYSTALS-Kyber-1024 was developed from a Python "Baby Kyber" model into full Verilog RTL, including a Keccak-f[1600]/SHAKE-128/256 XOF engine, a Centered Binomial Distribution noise sampler, a unified Cooley-Tukey/Gentleman-Sande NTT butterfly engine, and Montgomery–Barrett modular arithmetic. VI. **Phase VI RISC-V Processor Design:** a custom 32-bit, 5-stage pipelined RV32I processor with hazard detection and data forwarding was designed as the secure host controller intended to orchestrate both cryptographic engines via memory-mapped I/O.
4	**Outcome** All AES-128/192/256 and AES-GCM hardware outputs matched the Python golden model and official NIST Known-Answer Test vectors exactly, verified through both ModelSim and Vivado functional and gate level simulation and live hardware execution on four FPGA platforms using UART/RealTerm. The final AES-GCM Hardware/Software co-design SoC, implemented on an Intel Cyclone V DE10-Standard board, achieves a maximum frequency of 211.46 MHz on DE10 standard (5CSXFC6D6F31C6N) and 232.85 MHz on PYNQ-Z1 (XC7Z020CLG400-1) FPGA and a sustained effective throughput of 27.06 Gbps while consuming only 1,359 Adaptive Logic Modules (≈680 logic slices) an area efficiency of 39.80 Mbps/slice that outperforms twelve external (2024 – 2026) published AES/AES-GCM FPGA implementations benchmarked in this work, decisively breaking the traditional area-versus-speed barrier. This result has been documented in a research article prepared for the journal Cryptography (MDPI, 2026). In parallel, the CRYSTALS-Kyber-1024 accelerator was verified cycle-accurately against its Python reference and demonstrated functional Key Generation, Encapsulation, and Decapsulation on the Cyclone V platform (≈4.0 ms, ≈3.0 ms, and ≈1.2 ms respectively), while the standalone 5-stage pipelined RISC-V RV32I core was fully synthesized and verified with working hazard-detection and forwarding logic together providing three silicon-proven building blocks for a complete quantum-safe System-on-Chip.
5	**Evidence (Theoretical Basis)**

	The work is grounded in NIST FIPS-197 (AES), McGrew–Viega Galois/Counter Mode (GCM) Specification (2004), NIST SP 800-38A (Block cipher modes of operation) , NIST SP 800-38D (GCM/GMAC), and the NIST Post-Quantum Cryptography standard for CRYSTALS-Kyber, together with a comprehensive literature review of quantum threats (Shor's and Grover's algorithms) compared with recent solutions AES-GCM and Crystal Kyber's implementations and FPGA cryptographic accelerator design. A clearly defined research gap the persistent "area-speed barrier" in FPGA AES/AES-GCM implementations, where high-throughput pipelined designs consume 1,600–5,900+ logic slices while area-optimized iterative designs collapse to under 1 Gbps motivated a systematic, seven-iteration design-space exploration. The final Hardware/Software co-design was rigorously benchmarked against twelve external state-of-the-art AES/AES-GCM FPGA implementations (2024–2026) spanning Xilinx and Intel devices, and the Kyber-1024 accelerator was separately benchmarked against four published Kyber FPGA implementations, confirming the competitiveness of the proposed architectures.
6	**Competitive Advantage or Unique Selling Proposition** This project resolves a well-documented trade-off in cryptographic hardware design area versus speed while additionally offering an open, quantum-resistant security stack. Its key competitive dimensions are detailed below.
a	**Attainment of any SDG** SDG 9 – Industry, Innovation and Infrastructure: The development of an indigenous, quantum-resistant hardware security solution strengthens national technological infrastructure by enabling secure financial, defense, and communication systems while promoting innovation in next-generation semiconductor technologies. SDG 8 – Decent Work and Economic Growth: The adoption of the open-source RISC-V Instruction Set Architecture (ISA) and open Electronic Design Automation (EDA) tools democratizes access to advanced semiconductor design, fostering local talent development, enhancing workforce capabilities, and driving sustainable economic growth within the hardware engineering ecosystem. SDG 11 – Sustainable Cities and Communities: The proposed security core enhances the resilience and trustworthiness of smart-city and critical IoT infrastructure by providing robust hardware-level security, ensuring the reliable and secure operation of connected urban services.
b	**Any Environmental Aspect** Offloading Key Expansion to the existing ARM HPS and using BRAM-based iterative AES-GCM logic instead of massive parallel/pipelined data paths lets the design occupy under 4% of the Cyclone V's logic fabric (680 slice-equivalents versus 1,600–5,974 slices in competing designs) directly reducing dynamic power draw and the silicon area required for equivalent throughput.
c	**Cost Reduction of Existing Product**

	The entire authenticated-encryption accelerator fits within a fraction of a mid-range SoC FPGA, removing the need for expensive dedicated cryptographic ASICs or oversized high-end FPGAs. Both the AES-GCM core and the RISC-V host are built on royalty-free, open standards (NIST algorithms, RV32I ISA), eliminating IP-licensing costs associated with proprietary processor cores or crypto co-processors.
d	**Process Improvement which Leads to Superior Product or Cost Reduction, Efficiency Improvement of the Whole Process** Prior architectures forced a choice between throughput and area: iterative/FSM designs in the literature achieved only 0.91–25 Gbps to stay compact, while fully pipelined designs reached higher speeds only by consuming 1,600–5,974 logic slices. By offloading Key Expansion to the HPS and keeping only the datapath and GHASH engine on programmable logic, this project's Hardware/Software co-design achieves 27.06 Gbps at just 680 slices the best area-efficiency (39.80 Mbps/slice) and high speed of 211.46 MHz among all thirteen architectures compared in this study.
e	**Expanding of Market share** The significant reduction in silicon area and implementation cost enables the deployment of secure hardware in cost and resource-constrained applications that were previously unable to justify high-throughput cryptographic accelerators. These include IoT gateways, smart metering systems, point-of-sale (PoS) terminals, portable medical devices, and other edge computing platforms. Furthermore, by integrating AES-256 GCM authenticated encryption with the CRYSTALS-Kyber post-quantum key encapsulation mechanism, the proposed SoC provides a highly reliable and future-ready hardware security solution. This hybrid cryptographic architecture delivers strong protection against both current cyber threats and emerging quantum-computing attacks, making it well suited for long-term deployment in security-critical applications.
f	**Capture New Market** Post-quantum-ready hardware is an emerging and largely unaddressed segment. This project delivers early, silicon-validated building blocks a high-throughput AES-GCM engine, a Kyber-1024 KEM accelerator, and an open RISC-V host positioning it for organizations preparing for NIST-mandated post-quantum migration, long-life critical-infrastructure devices, and defense-grade communication systems requiring crypto-agility.
g	**Any Other Aspect** The complete hardware stack (RISC-V + AES-GCM + Kyber) is built entirely on open, non-proprietary standards, avoiding vendor lock-in and enabling independent third-party security auditing a critical requirement for government, defense, and financial-sector trust.
7	**Target Market**

	The proposed solution serves a diverse set of stakeholders across sectors where quantum-resistant, high-throughput secure communication is critical. The primary target markets include: I. Telecommunications operators, IoT/embedded-security vendors, and cybersecurity hardware firms seeking quantum-resistant accelerators for their products. II. Government, defense, and financial-sector organizations that must begin migrating to post-quantum cryptography to defend against "harvest-now, decrypt-later" threats. II. Semiconductor and SoC/FPGA developers and system integrators building secure edge, IoT, and industrial-control nodes. V. Academic and research institutions working on post-quantum cryptography, RISC-V security extensions, and FPGA-based cryptographic hardware.	
8	**Team Members** (Names along with email address)	Naveed Ahmed Siddiqui *(Team Lead)* (TC-22042) siddiqui4506165@cloud.neduet.edu.pk Syeda Zainab Bukhari (TC-22022) bukhari4501741@cloud.neduet.edu.pk Zainab Dawood (TC-22010) dawood4530462@cloud.neduet.edu.pk Taimoor Ali (TC-22030) ali4530428@cloud.neduet.edu.pk
10	**Supervisor Name** (along with email address)	Dr. Muhammad Fahim ul Haq mfahim@cloud.neduet.edu.pk
11	**Video (If any)**	N/A
12	**Pictures** (Pasted Below)	

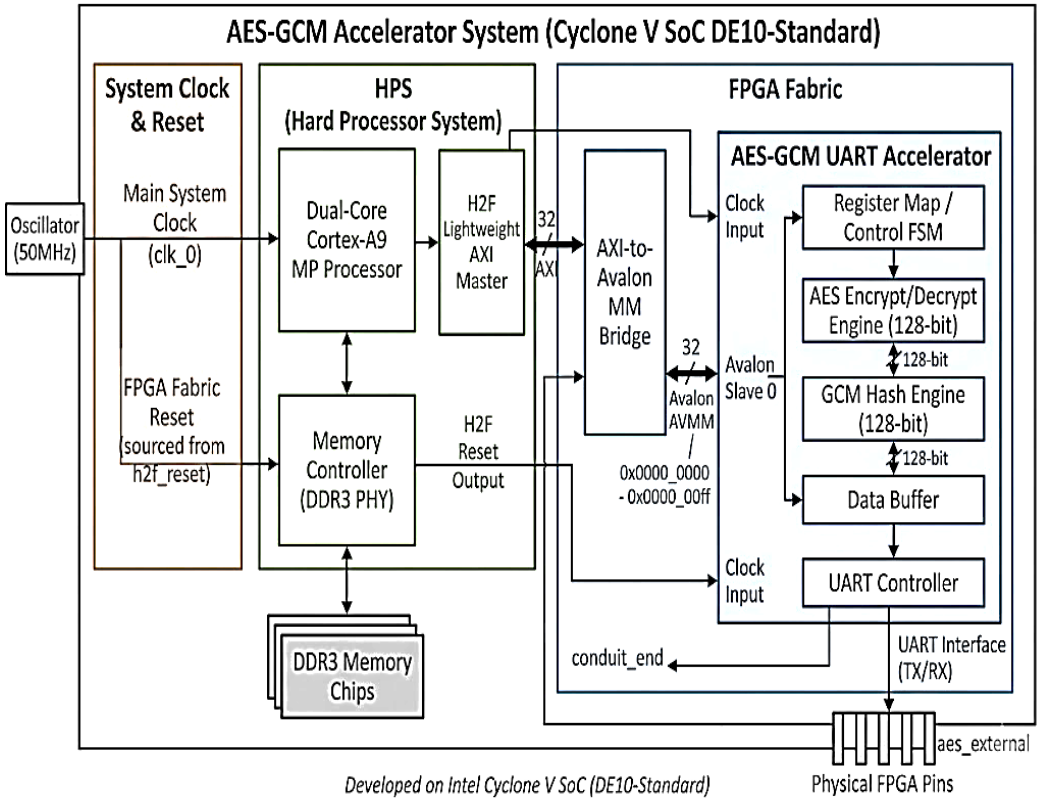
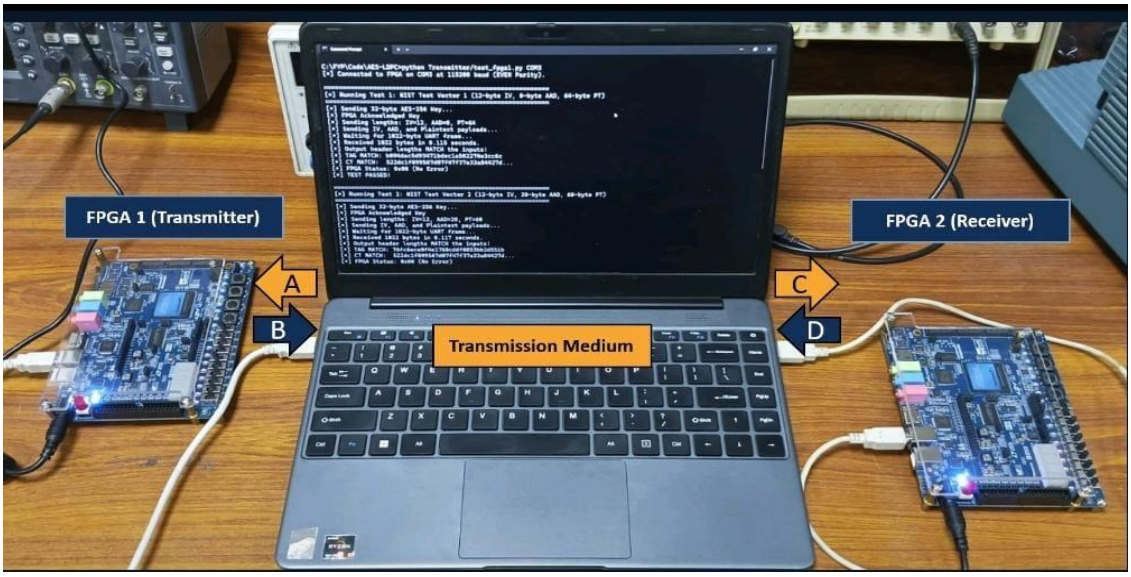


Figure 1 SoC (System on Chip) AES-GCM Hardware Architecture Integrated with



Cortex-A9

Figure 2: Complete Real-Time Hardware Test Setup (FPGA + UART + RealTerm)

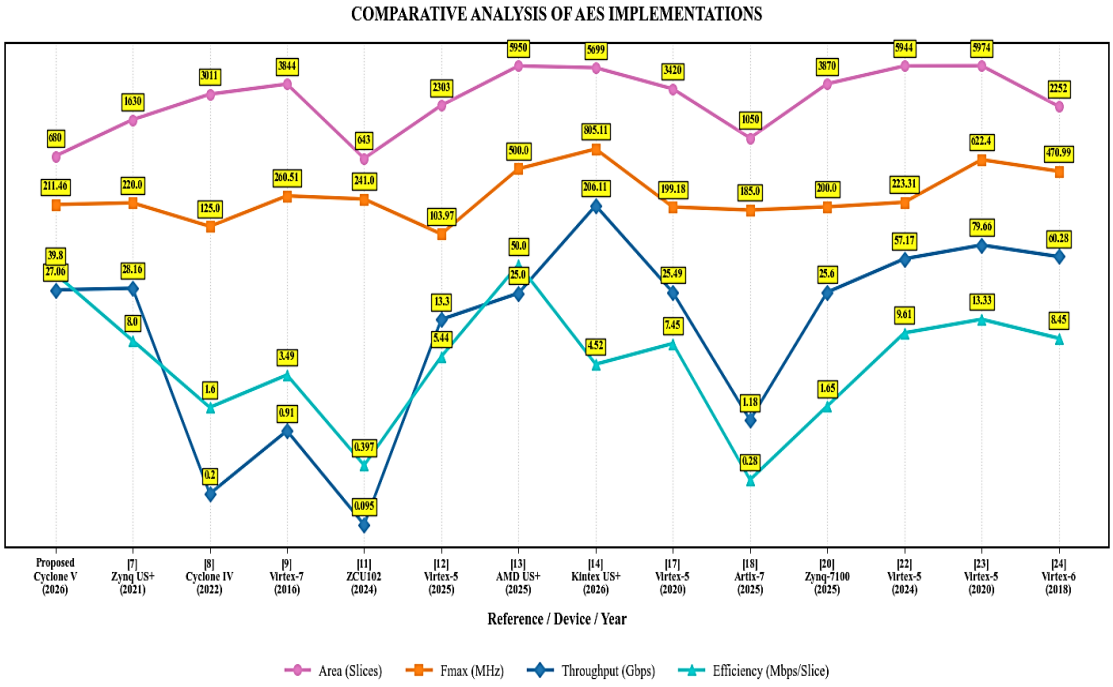
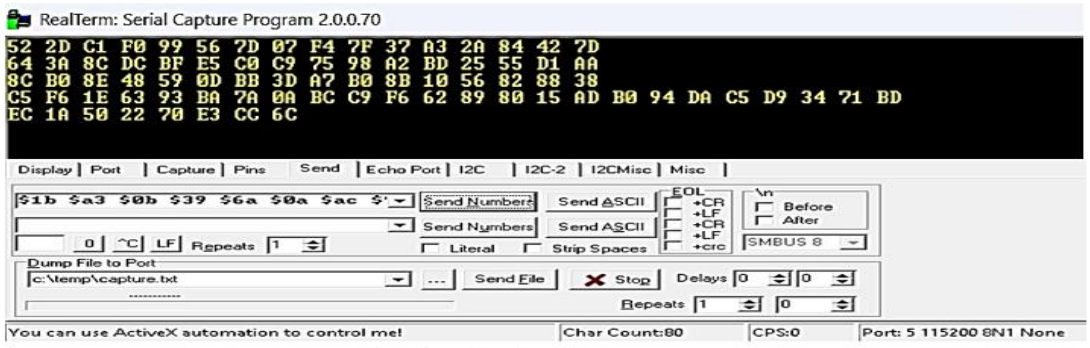
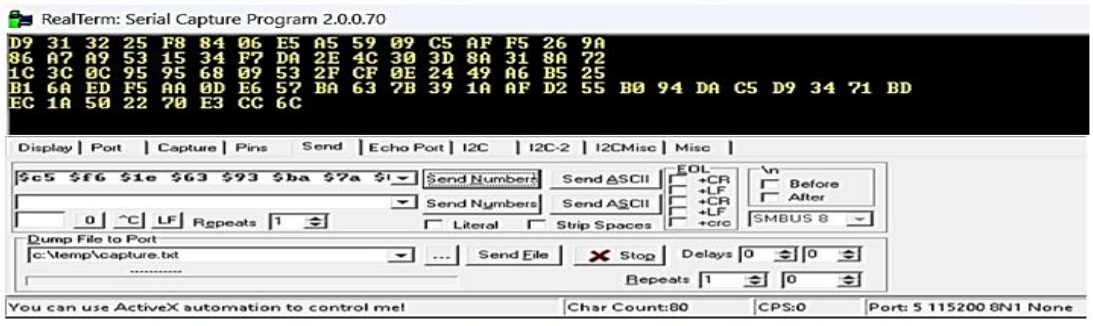


Figure 3: Comparative Area / Speed / Efficiency Analysis Against 12 External Published AES-GCM Implementations



RealTerm outputs showing live hardware Encryption for AES-256



RealTerm outputs showing live hardware Decryption for AES-256

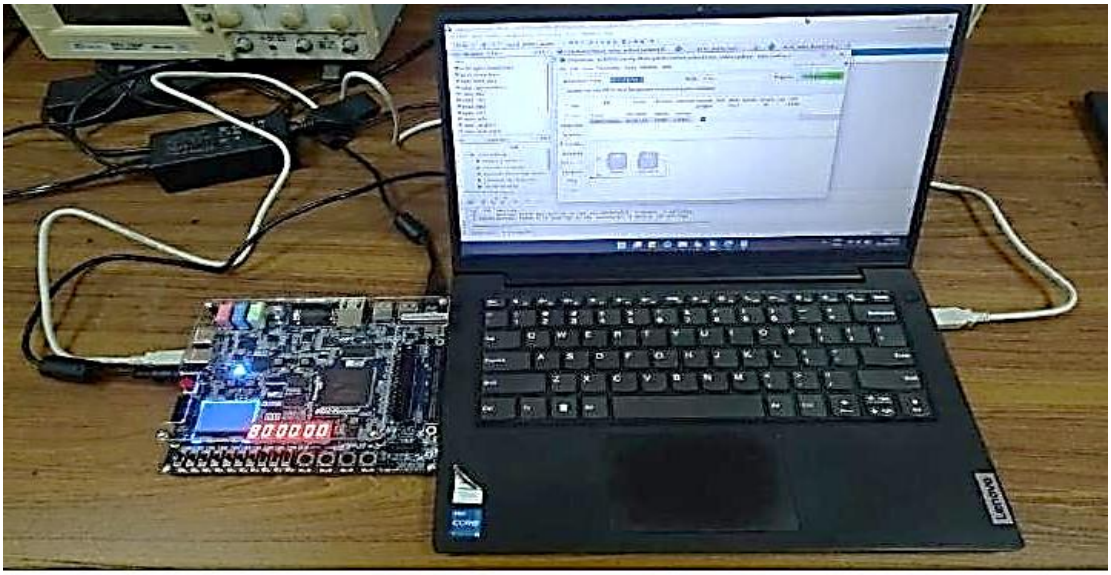


Figure 4 : Live implementation outputs on RealTerm terminal via UART of FPGA integrated with AES-GCM results verified with NIST test vectors.

Figure 5: CRYSTALS-Kyber-1024 Hardware Implementation on the DE10-Standard SoC Board