END-TO-END INTEGRATED CIRCUIT DESIGN

An Advanced Encryption Standard (AES) Core Implementation

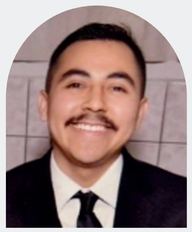
SDSU College of Engineering

Motivation

Currently, a vast majority of application-level encryption for passwords and sensitive information relies on software integration. While software implementation allows for flexibility, it is also limited to slower execution speeds and is more prone to software-based vulnerabilities, such as memory leaks and side-channel attacks. By designing a hardware-based cryptographic system to handle the encryption and decryption of sensitive information, it not only provides faster processing speeds, but also gives an isolated and secure environment for these operations, reducing the attack surface compared to standard software-based implementations.

The Nand5 Team

Monica Michael
Computer Engineering
Team Lead



Angel Martinez
Computer Engineering

Hector Ramirez
Computer Engineering

Sydney Kim
Computer Engineering

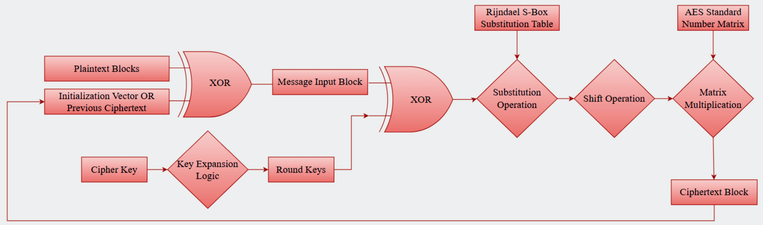
Matthew Chang
Electrical Engineering

Acknowledgements

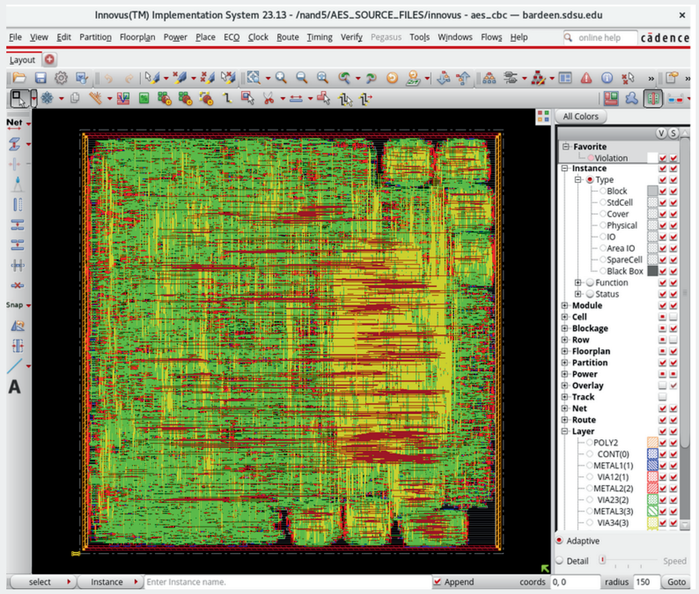
We would like to sincerely thank our sponsor, Dr. Ke Huang, for his support and insight, which were instrumental in the success of this project. The team would also like to thank Dr. Christopher Paolini for his guidance throughout Senior Design, and for providing the team access to the EDA tools used, among other resources that made this project possible.

Project Overview

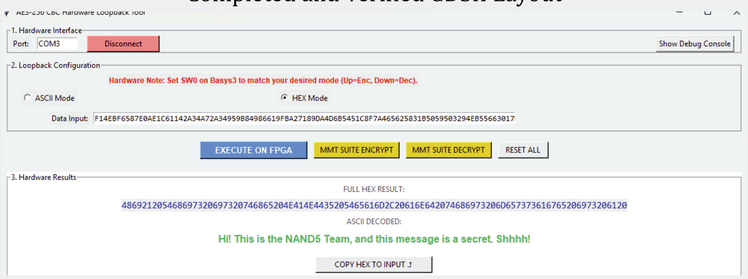
Our senior design team implemented a fully tapeout-ready AES-256 CBC encryption/decryption core using the TSMC 180nm PDK, completing the full RTL-to-GDSII ASIC design flow including synthesis, place-and-route, DRC/LVS verification, and post-layout simulation. In parallel, we developed an FPGA-based prototype enabling secure communication with a laptop through a custom GUI and driver software. The system demonstrates practical hardware cryptography and secure hardware integration inspired by Trusted Platform Module (TPM) architectures.



System Level Diagram of the AES Core Encryption Logic



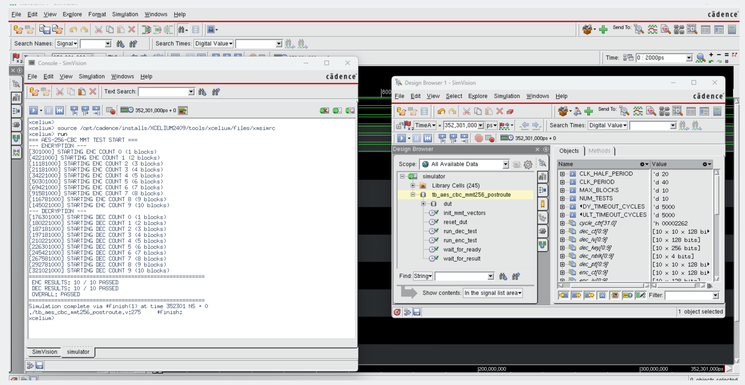
Completed and Verified GDSII Layout



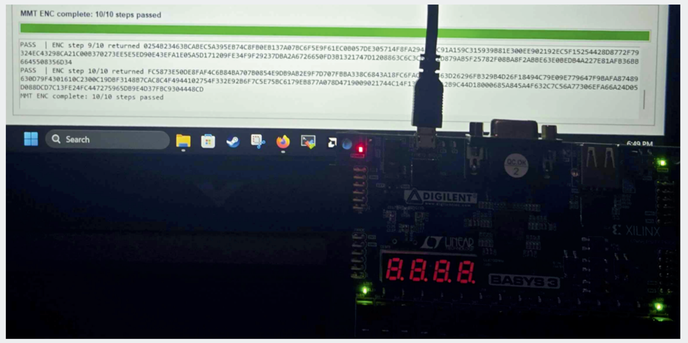
FPGA Demonstration Interfacing With Host PC Using Custom-Built GUI

Testing and Verification

The design test plan validates the AES core using standardized test vectors from NIST's AES Algorithm Validation Suite (AES-AVS), focusing on Known Answer Tests (KATs) and Multiblock Message Tests (MMTs) to ensure functional correctness for both single-block and chained (CBC) operations. Testing is performed in three phases: RTL simulation with self-checking testbenches, post-synthesis ASIC verification with reduced vector sets due to computational constraints, and FPGA prototype validation through a USB/UART interface with a GUI demo.



Final post-layout ASIC verification using MMT testbench in SimVision proving functional correctness under extracted physical timing delays. The test confirmed 100% compliance with the NIST-established MMT.



FPGA demonstration system test also shows 100% compliance with MMT.

Conclusion

Our team designed and implemented a tapeout-ready AES-256 CBC encryption/decryption system, validated with an FPGA prototype and software interface. The project demonstrates secure cryptographic operation and seamless hardware–software communication via UART and a GUI. Through this work, we gained experience in hardware design, system integration, and debugging, while showcasing practical embedded security applications.

Spring 2026