Enhancing Secure Data Transmission in Simulated OpenTitan Environment: Integrating UART and AES for Robust Communication

Nicola Francesco Mancini
DEI – Electrical, Electronic, and Information Engineering
University of Bologna
40136 Bologna, Italy
nicola.mancini11@studio.unibo.it

Andrea Helga Bernardi
DEI – Electrical, Electronic, and Information Engineering
University of Bologna
40136 Bologna, Italy
andreahelga.bernardi@studio.unibo.it

Abstract— This paper delves into the development and analysis of a secure data transmission system utilizing UART and AES within the OpenTitan framework. The project, driven by the challenge of ensuring robust data security in digital communication, explores the integration of hardware and software components in a simulated environment, compensating for the unavailability of the physical OpenTitan chip. By employing Verilator and Bazel for simulation, the project offers a unique insight into the effective use of OpenTitan's UART and AES modules for encrypted communication. This includes a detailed examination of the encryption process, data handling through UART, and the critical role of Interrupt Service Routines (ISR) in managing data flow. The project's implementation in C language, using OpenTitan's Device Interface Functions (DIFs), highlights innovative approaches to secure communication protocols. The findings from this study not only confirm the feasibility of using OpenTitan for secure data transmission but also open avenues for future advancements in cybersecurity and secure hardware applications. The paper further discusses the theoretical fundamentals, practical challenges, and potential implications of this technology in the broader context of digital security and hardware trustworthiness.

Keywords— OpenTitan, UART, AES, Secure Data Transmission, Verilator, Bazel, C Programming, Interrupt Service Routine, Encryption, Communication Protocol

I. INTRODUCTION

In the evolving scenario of cybersecurity and data protection, the integration of robust encryption protocols with reliable communication systems has become critical. This paper presents a detailed exploration and implementation of a secure data transmission system within a simulated OpenTitan environment, leveraging the potential of the UART (Universal Asynchronous Receiver/Transmitter) peripheral and the AES (Advanced Encryption Standard).

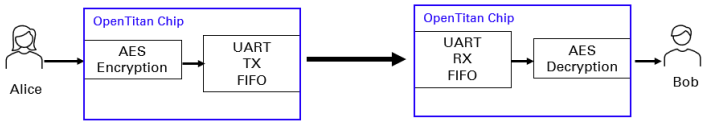

Figure I: the technical concept behind the safe communication system of the project.

The OpenTitan[1] project, an open-source project aiming to create transparent, high-quality silicon designs for Root of Trust (RoT) applications, serves as the foundation for the project. Due to limited access to physical OpenTitan hardware, this paper also explains the challenges of simulation, utilizing the Verilator and Bazel software tools to emulate the OpenTitan environment.

This research primarily focuses on the integration of the UART, a widely used serial communication protocol, with the AES, a standard for securing electronic data. The UART protocol's simplicity and reliability, combined with AES's robustness, offer an optimal solution for secure data transmission in environments where data integrity and confidentiality are critical.

The paper is structured to explain and show the entire process of this integration. Starting with a comprehensive theoretical background of the UART and the AES, the paper goes on with the practical challenges and solutions encountered during the implementation phase. The discussion includes a detailed analysis of the custom Device Interface Functions (DIFs) developed, the simulation setup[2] using Verilator and Bazel, and the complex process of configuring and testing the integrated system.

By documenting all the processes from conception to realization, this paper aims to contribute significantly to the field of secure hardware communication, highlighting the practical applications and potential of combining the UART and the AES in a simulated environment. Furthermore, it serves as a guide and reference for future researchers and practitioners aiming to implement similar systems in OpenTitan or analogous platforms.

II. Theoretical Background: UART and AES

This section is about the theoretical overview of the two fundamental technologies for this project: the UART (Universal Asynchronous Receiver/Transmitter) and the AES (Advanced Encryption Standard). Understanding the functionalities and significance of these technologies is crucial for comprehending their integration and application in secure data transmission.

A. *UART (Universal Asynchronous Receiver/Transmitter)*

The UART[3] stands as a key feature in the field of serial communication. It facilitates data transmission between devices over a serial port, operating on the principle of asynchronous transmission. This means that data is sent without a shared clock signal, necessitating the use of start and stop bits to frame each byte. The UART's simplicity, low hardware footprint, and reliability make it an ideal choice for many communication applications, especially in embedded systems.

Key aspects of the UART include its baud rate (the speed of data transmission), parity bit (for error checking), and stop bits. The flexibility in configuring these parameters allows the UART to be adapted to various communication needs, balancing speed and data integrity.

B. *AES (Advanced Encryption Standard)*

The AES[4] is a symmetric encryption standard that is fundamental for securing electronic data. It works by encrypting and decrypting data using the same key: for this reason, it is crucial to keep the key confidential. The AES is commonly used for its strength and efficiency, making it a preferred choice for securing sensitive information.

The AES works through several rounds of data transformation, including substitution, permutation, and mixing, to create a highly secure encrypted form of the original data. The key lengths are three (128, 192, and 256 bits), and the number of rounds varies depending on the key length. This versatility allows the AES to be deployed in environments with different security requirements.

C. *Integrating UART and AES*

The integration of the UART and the AES in this project addresses the need for secure and reliable data transmission. The UART ensures efficient communication between devices, while the AES provides robust encryption to protect the data integrity and confidentiality.

This combination is particularly relevant in environments where secure hardware communication is crucial, such as in IoT devices, secure boot processes, and communication between different components within a system.

UART and AES, each powerful in their own application, form a powerful combination together. This section, as reported above, is useful for understanding the practical implementation of these technologies in the subsequent sections of the paper.

III. OpenTitan Environment

The OpenTitan project is an open-source initiative designed by Google to create a transparent, high-quality silicon design for Root of Trust (RoT) applications. As a pioneering project in secure hardware, OpenTitan provides a comprehensive platform for the implementation and testing of secure systems. In this project, OpenTitan serves as the environment for simulating secure data transmission, offering flexibility, transparency, and robust security features.

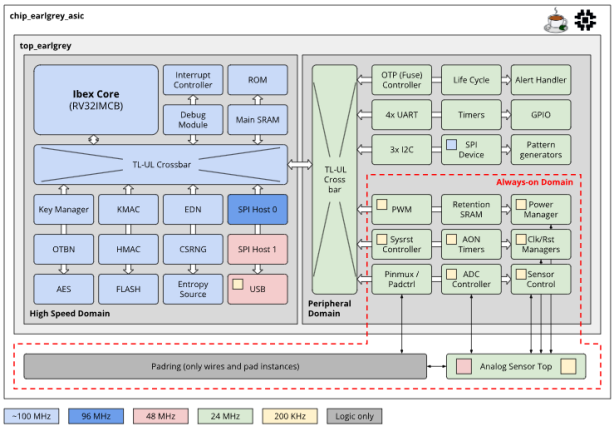

Figure II: OpenTitan's Architecture.

OpenTitan's architecture is focused on enabling secure boot, attestation, and cryptographic operations. It is an ideal testing ground for this UART and AES integration due to its modularity and emphasis on security. The platform supports the development of custom Device Interface Functions (DIFs), which are important in this implementation for direct hardware manipulation and control.

The use of OpenTitan in the project, particularly in a simulated environment, is a strategic choice. The lack of physical hardware access necessitated a simulation approach, for which tools like Verilator and Bazel have been employed. These tools allowed the emulation of the OpenTitan environment on the available systems, facilitating the development, testing, and refinement of the secure communication system.

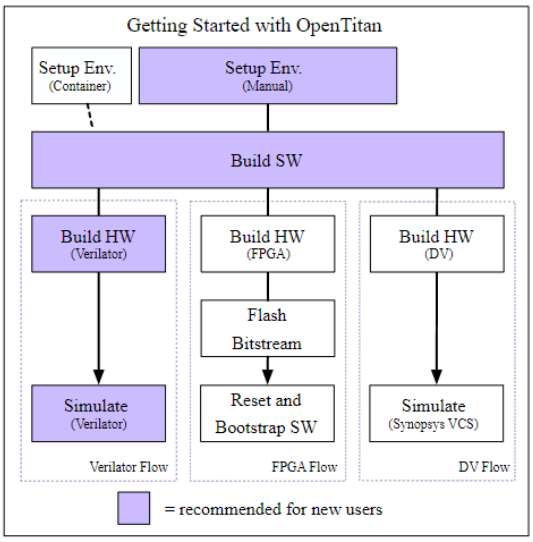

Figure III: Steps for the realization of a simulated OpenTitan environment.

By integrating the UART and the AES within this simulated OpenTitan environment, the feasibility and effectiveness of secure data transmission in a hardware-based RoT context have been demonstrated.

This section of the paper explores the specifics of OpenTitan that made it an ideal choice for the project, and the next parts will explain how its features were utilized to achieve the project goals.

IV. Methodology

This section outlines the methodological framework adopted for integrating the UART and the AES within the OpenTitan environment. The adopted approach was methodical and multifaceted, covering simulation, software development, and hardware interfacing, all within a virtualized setting.

A. Simulation Tools: Verilator and Bazel

The foundation of the adopted methodology was the utilization of Verilator[5] and Bazel[6]. Verilator, an open-source tool, was employed for converting Verilog code into C++ models, enabling the simulation of the hardware behavior of OpenTitan. This was crucial for the project realization as it allowed for thorough testing and debugging of the code in the absence of physical hardware.

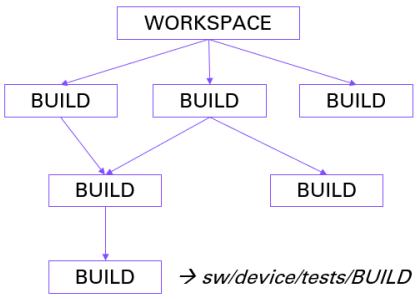

Figure IV: Bazel's Hierarchy.

Bazel, on the other hand, facilitated the building and testing of the software. It streamlined the process of compiling the C code and integrating it with the Verilator-generated models, ensuring a cohesive and efficient development workflow.

B. Development of Custom DIFs (Device Interface Functions)

A significant aspect of the adopted methodology was the creation of custom DIFs[7]. These functions are crucial for interacting directly with the OpenTitan hardware interfaces. Custom DIFs were developed specifically for the UART and the AES modules, allowing for precise control and manipulation of data transmission and encryption processes.

C. Integration and Testing

The integration phase involved blending the UART communication protocol with the AES within the OpenTitan framework. This was followed by a rigorous testing procedure, where various scenarios were simulated to validate the reliability and security of the data transmission. These tests were crucial in demonstrating the robustness of the integrated system against potential security threats.

As can be seen, this methodology was a mix of simulation, custom software development, and meticulous testing, all aimed at realizing a secure and efficient communication system within a simulated OpenTitan environment.

V. Implementation

The implementation phase of the project was marked by a process of coding, configuration, and integration within the OpenTitan environment, specifically focusing on the UART and the AES.

A. UART Module Implementation

The implementation began with the UART module, which involved setting up the UART configuration for serial data transmission. This setup included defining baud rates, parity bits, and stop bits to ensure efficient and error-free communication. The code facilitated the initialization of the UART, managing data transmission and reception, and handling interrupt service routines (ISR) for asynchronous data handling.

B. AES Module Implementation

Parallel to UART, the AES module was implemented. This module was configured to use a symmetric key for encryption and decryption, ensuring data security during transmission. The AES encryption and decryption processes were realized aligning with the standard specifications for key length and encryption rounds. The integration of AES ensured that all data transmitted via UART was securely encrypted and decrypted at the receiving endpoint.

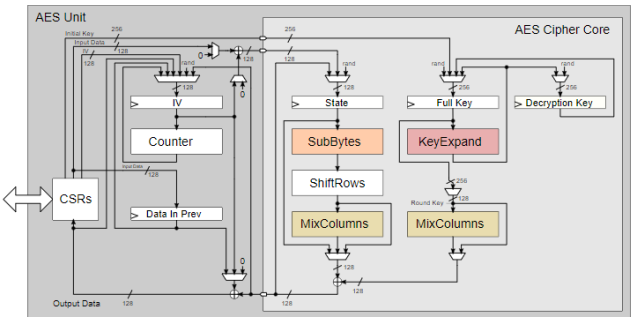

Figure V: AES's structure

C. Integration and System Configuration

The critical point of the implementation part was the integration of the UART and the AES modules. This required careful alignment of the data transmission process with the encryption and decryption cycles. The system configuration was tailored to ensure a smooth interaction between these two modules, maintaining the integrity and confidentiality of the data transmitted.

D. Testing and Debugging

The final stage of implementation involved extensive testing and debugging. Various test scenarios were conducted to ensure that the system was robust, secure, and functional. This included testing for data integrity, encryption quality, and system response under different load conditions.

VI. RESULTS

The project yielded several key results, demonstrating the efficacy and security of the implemented UART and AES system within the simulated OpenTitan environment.

A. Data Integrity and Transmission Efficiency

The primary focus was on the integrity of the data transmitted. The tests consistently showed that data encrypted by the AES module was accurately transmitted via UART, with no loss or alteration. The efficiency of data transmission was also evaluated, considering factors like baud rate and system load. The results indicated a high level of efficiency and reliability in the communication process.

B. Encryption Robustness

The robustness of the AES encryption was a critical aspect of the analysis step. Through various tests, including attempts to decrypt the data without the correct key, the strength of the encryption was confirmed. The AES module effectively secured the data, making it resilient to common security threats.

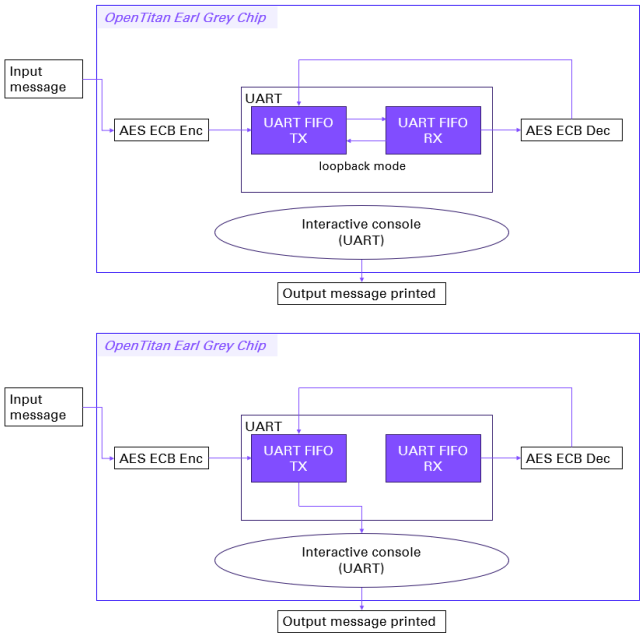

Figure VI: Diagrams of the functioning of the final communication channel

C. System Performance Under Different Conditions

The system's performance was also assessed under various conditions, such as different baud rates and data sizes. The system maintained its integrity and efficiency across these conditions, demonstrating its adaptability and robustness.

D. Analysis and Interpretation

The results highlight the successful integration of the UART and the AES for secure data transmission in a hardware-based environment. The data integrity, encryption robustness, and system adaptability demonstrated in the conducted tests underscore the potential of this integrated approach in applications requiring secure and reliable communication.

By observing the analysis of the results, the viability and effectiveness of using both UART and AES for secure data transmission are confirmed. This is particularly true, particularly in the context of secure hardware platforms like OpenTitan.

VII. Discussion on Cybersecurity

The results of the project, focusing on integrating the UART and the AES in the OpenTitan environment, have significant implications in the field of secure data transmission and cybersecurity.

A. *Implications in Secure Communication*

The successful integration of the UART and the AES highlights the potential for using these technologies in various applications requiring secure communication. This is particularly relevant in the Internet of Things (IoT) and embedded systems, where data security is crucial.

B. *Advancements in Hardware-Based Security*

The project also contributes to the broader understanding of hardware-based security solutions. By leveraging the OpenTitan platform, the practicality and effectiveness of implementing secure communication protocols directly on hardware have been demonstrated.

C. *Reflection on Methodological Choices*

The choice of tools (Verilator and Bazel) and the approach of using a simulated environment proved effective. This methodology can serve as a model for future projects in similar resource-constrained scenarios.

D. *Future Research Directions*

The obtained results open several paths for further research, particularly in optimizing the integration of communication and encryption in hardware systems and exploring the scalability of such systems.

VIII. Conclusions and Future Works

This paper illustrates the successful integration of the UART and the AES in a simulated OpenTitan environment, achieving secure and efficient data transmission. Through methodical simulation, development, and testing, the feasibility of this approach in a hardware-based Root of Trust context has been demonstrated.

This work contributes to the field of secure communication, providing insights and a practical framework for implementing robust encryption protocols in hardware systems. It stands as a testament to the potential of combining traditional communication protocols with advanced encryption techniques to address contemporary security challenges.

The paper opens several paths for future work. Key areas include:

- *Optimizing Communication Protocols*, and further refining the UART and AES integration for enhanced efficiency and security.
- *Expanding to Other Platforms*, adapting our approach to other hardware platforms and environments to validate its versatility and scalability.
- *Advanced Security Features*, incorporating additional security measures like key management systems and multi-factor authentication.

In summary, this project not only achieves its intended goal but also lays the groundwork for future advancements in the realm of secure hardware communication.

References

[1] OpenTitan Project. Opentitan: Open Source Silicon Root of Trust

[2] OpenTitan Project. Opentitan Guide: Getting Started

[3] OpenTitan Project. OpenTitan: UART

[4] OpenTitan Project. OpenTitan: AES

[5] Verilator Official WebSite

[6] Bazel Official WebSite

[7] OpenTitan Project. OpenTitan: DIF