CHIP-LEVEL INTEGRATED TECHNOLOGY FOR ADVANCED DEFENSE AND ENCRYPTION LAYER

submitted to
Prof. Michael Taylor
Paul Gao
Elpida Karapepera

by

Eric Yu, Oliver Cao
University of Washington

Table of Contents

Abstract

In the heart of the digital age, where every pulse of data traverses intricate pathways, a silent battle rages—a battle for security, for trust, for the sanctity of information. The risks of hardware backdoors loom large, casting shadows on the integrity of our interconnected systems, and processing an eminent danger for data breaches which could lead to potential chaos in society. The Chip-Level Integrated Technology for Advanced Defense and Encryption Layer (CITADEL) project is tasked to build a world where the very fabric of communication is fortified, where each chip pulsates with an unyielding shield against malevolence. The ASIC design, meticulously woven with the Advanced Encryption Standard (AES) and emboldened by a 256-bit key length, transcends mere performance metrics. It is a sentinel—an auditable, transparent guardian of data. The project defies the shroud of secrecy that often veils commercial chips, opting instead for openness. CITADEL's commitment echoes through the corridors of shared knowledge, where BaseJump STL beckons collaboration.

A. Introduction

A.1. The Problem

In the contemporary landscape of technology, where custom chip designs are flourishing and inter-chip communications are increasingly prevalent, the sanctity of data security has never been more critical. The semiconductor chips, which form the backbone of our digital infrastructure, are now ubiquitous, finding their place in everything from critical infrastructure to consumer electronics. However, this widespread deployment comes with heightened risks; chip-based hardware backdoors have emerged as a severe threat, enabling espionage, data theft, and sabotage on a scale previously unimaginable, all while circumventing conventional security protocols. Recent studies highlight the alarming concerns over such vulnerabilities, with an estimated 2,220 cybersecurity incidents reported in 2023 alone, where backdoor deployment was the top action attackers made in almost a quarter of all incidents remediated in recent years [1]. This underscores the imperative need for secure and resilient chip designs that can withstand the evolving landscape of cyber threats.

A.2. The Solution

The development of the CITADEL project is a direct response to the growing threats posed by hardware backdoors and the critical need for secure data transmission [2]. The project embodies a commitment to transparency and leverages an open-source approach to chip design, which is essential for enhancing data security in the realm of inter-chip communications [3]. At the core of CITADEL is the Advanced Encryption Standard (AES), a symmetric encryption algorithm celebrated for its robustness and efficiency [4]. By implementing AES in a hardware-centric manner, CITADEL ensures high-speed data encryption. This hardware-centric implementation not only boosts performance but also surpasses the physical security measures of software-based encryption solutions.

CITADEL's foundation on the open-source BaseJump-STL framework is a strategic choice that underscores the project's dedication to transparency. It allows every component of the chip design, from the sophisticated encryption algorithm to the intricate circuits, to undergo rigorous auditing and verification by independent entities. This level of openness is pivotal for building trust in the chip's security capabilities and promotes a collaborative environment for advancing secure chip design. The project's approach is a stride towards a future where data security is ingrained in the fabric of every chip, ensuring a safer technological ecosystem for all.

A.3. Usefulness and Novelty

The CITADEL project marks a significant stride in the domain of data encryption, providing enhanced security and efficiency. CITADEL adopts a holistic approach, accommodating a wide array of applications by prioritizing high-throughput capabilities with a substantial 256-bit key length. This robust key length is not merely a technical upgrade; it represents a strategic defense against the complex cyber threats that characterize our digital era.

The project's novelty is highlighted by its divergence from the non-transparent practices prevalent in commercial chip design, where essential functionalities are often hidden behind Non-Disclosure Agreements (NDAs), compromising transparency and potentially leading to less-than-optimal hardware implementations [5]. CITADEL, on the other hand, champions openness and collective progress. It is grounded in the shared-knowledge ethos of platforms like BaseJump STL, contributing to the ever-growing pool of open-source hardware designs. This dedication to openness goes beyond philosophy to practical application, fostering ongoing peer review and continuous enhancements. The project's progress is thoroughly documented and shared for community engagement, democratizing innovation and catalyzing a collaborative development environment.

In essence, CITADEL is not only a technical endeavor but also a cultural shift in chip design, advocating for transparency, collaboration, and community-driven progress. It exemplifies the transformative impact of the open-source philosophy within the semiconductor industry, heralding a future where security and efficiency are seamlessly integrated with accessibility and collective intelligence. The project's usefulness is underscored by its potential to safeguard critical information exchanges across various sectors, including aerospace, defense, finance, and healthcare—industries that handle sensitive data requiring protection from unauthorized access and cyber threats. By implementing robust end-to-end encryption with the AES-256 algorithm, CITADEL ensures the secure encryption of data transmitted between chips, mitigating the risks of data breaches and unauthorized access.

B. Technical Background

B.1. State of the Art

In the ever-evolving realm of chip-to-chip communication security, the research community is actively addressing the intrinsic vulnerabilities present in Network-on-Chip (NoC) systems within System-on-Chip (SoC) architectures. The

distributed nature of NoCs renders them prone to security infringements, thus propelling the development of sophisticated countermeasures to safeguard SoCs against hazards such as unauthorized data access and service disruptions [1]. In this context, the CITADEL project has strategically chosen the robust AES-256 encryption standard to enhance inter-chip communications security.

AES-256 is distinguished as a symmetric encryption paradigm, renowned for its exceptional security and operational efficacy. It manipulates 128-bit data blocks with a 256-bit key, ranking it among the most secure encryption methods available [1]. The encryption routine is an intricate sequence of substitution, transposition, and mixing, transforming plaintext into encrypted ciphertext with precision. Notably, AES-256's quantum resistance is akin to AES-128's defense against traditional cyber threats, making it an optimal safeguard for sensitive data against both existing and emergent cryptographic challenges [4].

CITADEL's implementation of the AES-256 algorithm is grounded in the open-source BaseJump-STL library. This collection of hardware primitives and modules is pivotal in refining the design process [6]. The bsg-link module, in particular, underscores the library's importance by offering high-speed off-chip communication capabilities, which are crucial for ensuring secure chip-to-chip data transfers[7]. The integration of BaseJump STL into CITADEL's framework not only simplifies the incorporation of AES-256 but also assures that the communication protocols withstand extensive testing and validation.

SkyWater 130 (SKY130) process has been selected as the foundational technology for the project. The proven 180nm-130nm hybrid technology made accessible through a collaboration between Google and SkyWater Technology Foundry. SKY130 provides designers with the tools necessary to create functional designs, representing a significant contribution to open-source advancements in ASIC development [8]. This decision demonstrates CITADEL's commitment to utilizing community-sourced resources to advance ASIC design, positioning the project at the forefront of technological innovation.

CITADEL's innovative approach in addressing chip-to-chip communication security is a significant stride towards fortifying the integrity of SoC architectures. By harnessing the power of AES-256 encryption and leveraging the open-source BaseJump-STL library, CITADEL fosters a culture of transparency and collaboration in ASIC design. The utilization of the SKY130 process underscores a commitment to accessible, cutting-edge technology, ensuring that CITADEL remains at the forefront of the industry. As the project progresses, it stands as a beacon of progress, embodying the principles of rigorous security, modular design, and community-driven innovation. Through such endeavors, CITADEL is poised to make a lasting impact on the future of secure chip-to-chip communication, paving the way for a safer and more reliable digital infrastructure.

B.2. Competition

In the dynamic realm of encryption technologies, CITADEL emerges as a trailblazer amidst a sea of innovative contenders. The software sector heralds the cryptography library as a beacon for developers, offering a rich Python toolkit replete with high-level constructs and low-level access to a suite of cryptographic algorithms. This includes the essentials: symmetric ciphers, message digests, and key derivation functions [9]. Its user-friendly nature and extensive documentation have cemented its status as the go-to resource for developers seeking to embed encryption into their applications seamlessly.

Venturing into the hardware territory, CITADEL stands shoulder to shoulder with initiatives such as AESHA32 and AES-Verilog. AESHA32 marries the AES algorithm with the SHA-3 hashing function in a Verilog incarnation, boasting an ASIC design that thrives on 0.18um technology. It operates at a peak frequency of 60 MHz within a compact 1.462 mm square chip, maintaining a modest power footprint of 0.53W [10]. In parallel, AES-Verilog offers a comprehensive Verilog HDL rendition of the AES protocol, accommodating AES128, AES192, and AES256. This project takes life in a DE1-SoC FPGA, albeit at a lower clock frequency of 50MHz [11]. These ventures are testaments to the open-source community's dedication to forging robust, hardware-centric encryption solutions that seamlessly blend into diverse systems.

What sets CITADEL's ASIC implementation apart is its unwavering focus on securing chip-to-chip communications, bolstered by superior performance metrics and optimized power and area considerations. By harnessing the SkyWater 130 process, CITADEL pioneers manufacturable designs and champions the open-source movement. With its deployment of AES-256, renowned for its resilience against quantum threats, CITADEL positions itself at the vanguard of encryption, ready to tackle both present and looming cryptographic challenges.

CITADEL's allegiance to security, performance, and the open-source creed distinguishes it in the competitive landscape. With an eye on the unique demands of secure inter-chip communication and the latest open-source advancements, CITADEL aspires to deliver a solution that is secure and efficient but also transparent and verifiable, echoing the industry's evolving needs and expectations.

C. Experimental Setup

C.1. Summary

The final deliverable for the CITADEL project is a state-of-the-art ASIC chip designed for high-security chip-to-chip communication. This chip will incorporate the AES-256 encryption standard, ensuring robust protection against quantum computing threats. CITADEL aims to provide a secure communication channel between chips, safeguarding data from interception or tampering. This setup aims to address the increasing need for security in transmitting sensitive information in various applications, from consumer electronics to critical infrastructure.

A comprehensive test harness will be developed to validate the functionality and performance of the CITADEL chip. This will include automated tests to verify the chip's encryption and decryption capabilities, power consumption, and operational frequency. The test harness will simulate real-world scenarios to ensure the chip performs as expected under different conditions. The test environment will also assess the chip's resistance to various attack vectors, confirming its security robustness.

In summary, the CITADEL project aims to deliver a secure, efficient, and open-source ASIC chip for encryption, accompanied by a robust test harness to demonstrate its effectiveness and reliability in securing chip-to-chip communication. The detailed design and testing approach will be meticulously documented to facilitate transparency and ease of replication in the open-source community.

C.2. The Setup

To realize the vision of the CITADEL project, a sophisticated ASIC chip has been devised, dedicated to ensuring secure chip-to-chip communication through AES-256 encryption. The project unfolds in three pivotal segments, as delineated in **Figure 1**. At the heart of CITADEL are the encryption and decryption modules, which form the linchpin of secure intra-chip dialogue. These modules will undergo stringent testing to affirm their operational integrity and reliability.

The initial phase of testing employs BaseJump's trace replay, where a vector file articulating the message and key for encryption, alongside the anticipated encrypted output, is meticulously crafted. This process draws upon the benchmark samples provided by the National Institute of Standards and Technology (NIST) [4]. Subsequently, the project harnesses contemporary testing frameworks like CocoTB, which facilitates a more automated and stochastic testing regime [12]. A Python script, leveraging cutting-edge software algorithms, computes the expected outcomes from inputs randomized by Python's native randomization utilities. CocoTB then dispatches these inputs to the hardware and juxtaposes the hardware's output against the software predictions. This rigorous testing protocol encompasses over 50,000 randomized trials, supplemented by an additional 1,000 tests derived from trace replay, to guarantee that both encryption and decryption functionalities align with the projected standards. The hardware simulation was carried out using the VCS simulator, ensuring a thorough and accurate representation of the modules' performance.

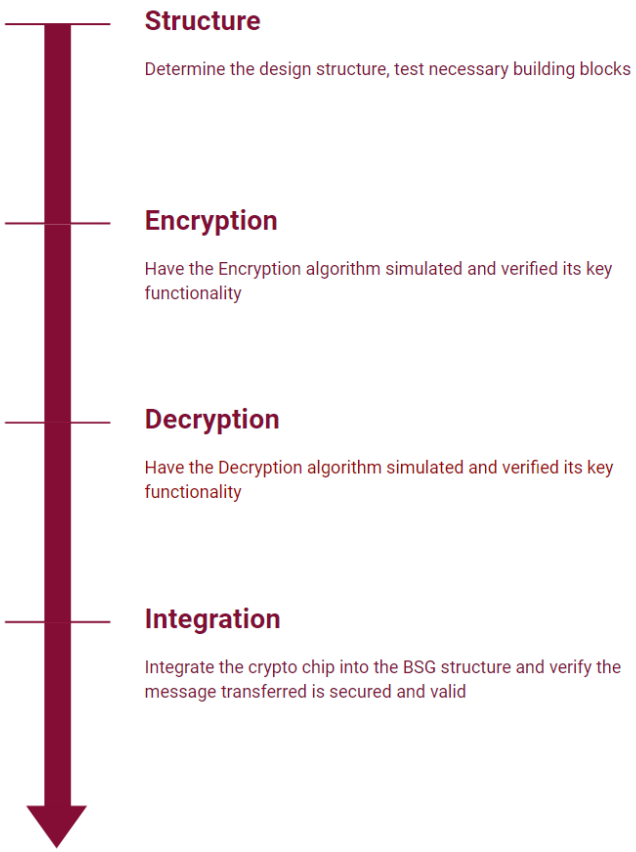

Figure 1. *Overall structure of the project*

To fulfill the overarching objective of secure inter-chip communications, CITADEL orchestrates a seamless integration of its encryption and decryption modules with the BaseJump-STL's bsg_link modules. As illustrated in **Figure 2**, the strategic placement of the encryption and decryption units precedes the bsg_link modules. This configuration is crucial for encrypting messages before they embark on their journey through the bsg_link, ensuring that every bit of data remains secure until it reaches the intended recipient. Upon delivery, the decryption module within the receiving chip's bsg_link swiftly reconstructs the message to its original form, ensuring the integrity of the data is preserved from end to end.

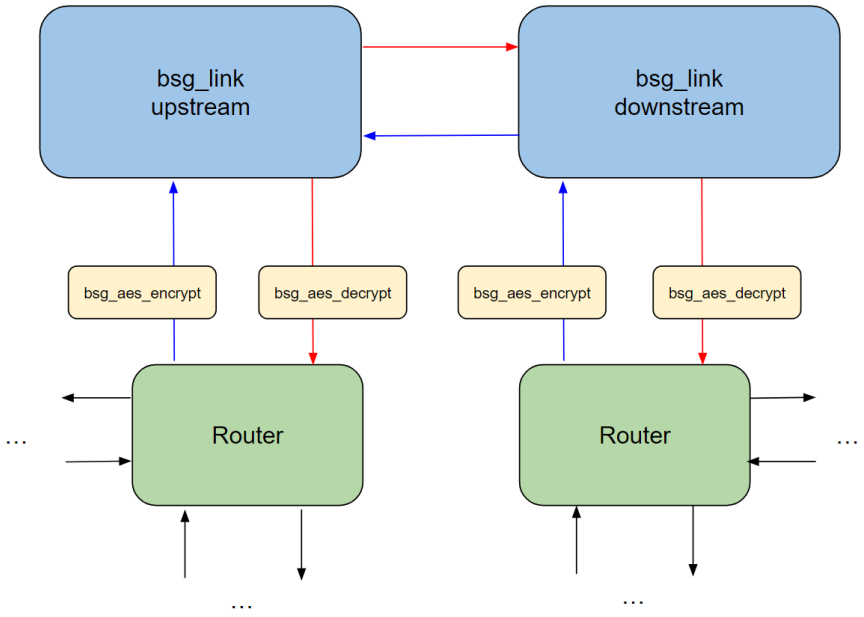

Figure 2. *The specific location of the encryption and decryption modules relative to the bsg_link modules*

C.3. Procedure

The CITADEL project's hardware implementation for encryption and decryption is predicated on the AES algorithm as specified by NIST [4]. The process begins with key expansion, where a 256-bit key is transformed into fifteen 128-bit expanded keys for subsequent encryption rounds, as shown in **Figure 3**. This expansion occurs over eight rounds, each accepting a 256-bit key from its predecessor and outputting a new 256-bit key for the next round, with the exception that the final round yields only 128 bits. Each round involves an XOR operation with the key and a substitution step using the S-Box ROM lookup table.

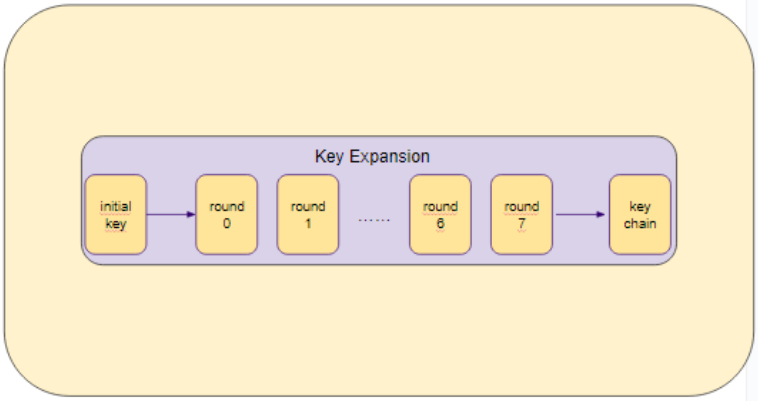

Figure 3. *High-level overview of the key expansion module*

Following key expansion, the resultant keychain feeds into fifteen distinct rounds of encryption. Each round commences with the add round key module, which performs an XOR operation between the key and the state, or the text being encrypted. The plaintext undergoes an initial round key operation, followed by thirteen rounds of sub-bytes, shift-row, mix-column, and another round key operation, executed in sequence. The final round omits the mix-column step to finalize the encryption. Each round's sub-bytes module substitutes the input message with corresponding S-Box values, akin to the key expansion phase. The shift-row module processes the 128-bit message in 32-bit segments, cyclically shifting each segment by 8 bits. Lastly, the mix-column module applies a transformation by shifting and XORing different bytes within the state. This meticulous procedure ensures a robust encryption process, securing the data as it moves from plaintext to ciphertext. **Figure 4** shows an overview of the encryption module

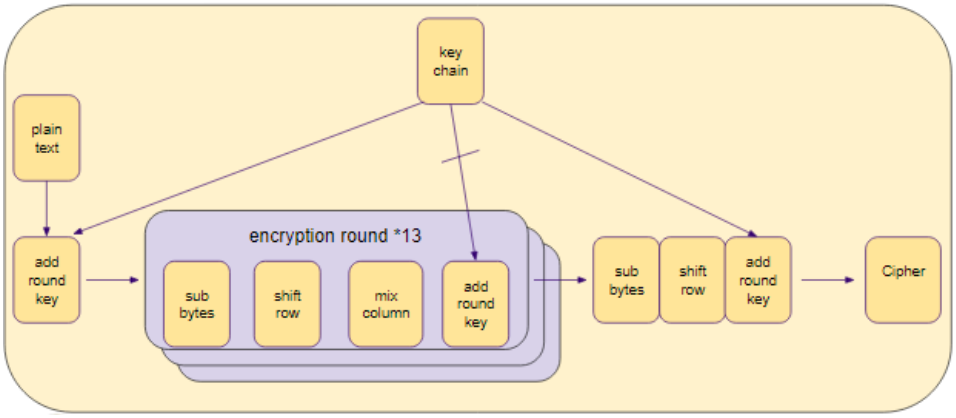

Figure 4. *High-level overview of the encryption module*

The decryption module is a sophisticated counterpart to the encryption mechanism, designed to reverse the AES algorithm's encryption. It processes a 128-bit encrypted message alongside a keychain of fifteen 128-bit expanded keys, navigating through phases that include add-round-key, inverse-sub-bytes, inverse-shift-rows, and inverse-mix-columns, as shown in **Figure 5**. The inverse-sub-bytes stage employs inverse S-Box ROMs for byte substitution, undoing the encryption's sub-bytes step. inverse-shift-rows follows, rotating 32-bit blocks of the state to their original positions, counteracting prior shifts. Concluding the process, inverse-mix-columns reverses the mix-columns operation, reinstating the bytes to their initial state. This decryption module ensures the encrypted message is accurately decrypted, restoring the plaintext and upholding the integrity of CITADEL's secure communication framework. The module's seamless integration within the project highlights CITADEL's dedication to providing robust cryptographic solutions.

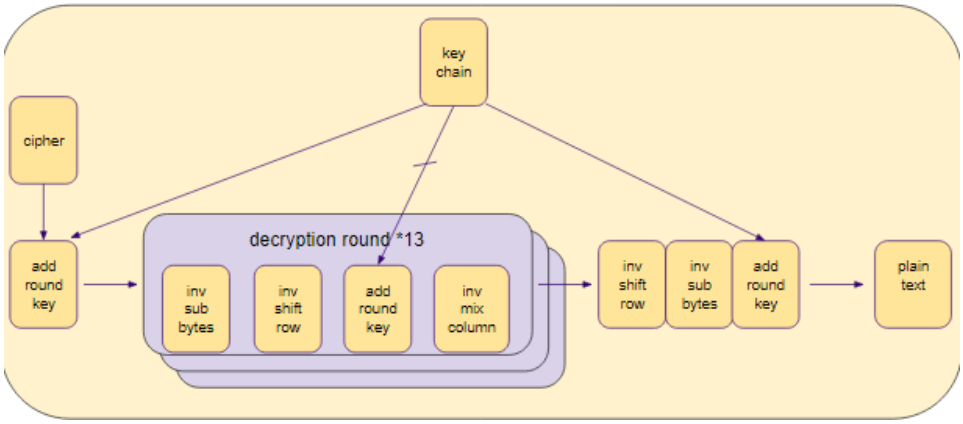

Figure 5. *Overall structure of the decryption module*

The seamless integration of CITADEL's encryption and decryption modules with BaseJump-STL is pivotal to achieving the project's ultimate goal of secure inter-chip communication. By implementing the valid-ready handshake protocol inherent to BaseJump-STL, CITADEL ensures that all data transactions are synchronized and validated [6]. As depicted in **Figure 6**, a dedicated control logic manages the handshake signals, coordinating the flow between modules. A strategically placed multiplexer discerns whether to retain the current data stream or to introduce a fresh dataset to the cryptographic modules. Subsequently, a register post-multiplexer captures and supplies the data to the encryption or decryption units, guaranteeing uninterrupted cryptographic operations. This integration not only fulfills CITADEL's stringent specifications but also exemplifies the project's commitment to precision and reliability in secure data exchange.

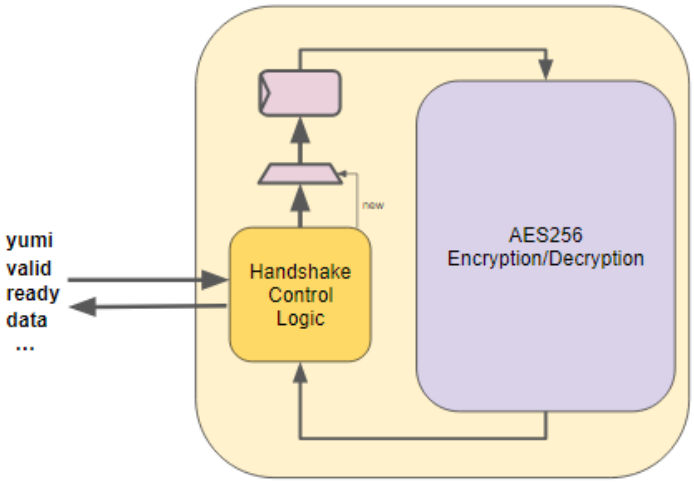

Figure 6. *BaseJump wrapper for encryption and decryption modules*

D. Results

D.1. Summary of the Results

The culmination of the CITADEL project is epitomized in the seamless integration of both encryption and decryption modules with the bsg_link module, nestled within the bsg_gut framework. The design process and rigorous testing have led to a robust top-level architecture, where the cryptographic modules coalesce with the communication infrastructure of a standard BaseJump chip. **Figure 7** provides a comprehensive chip-level representation of this integration, showcasing the harmonious interplay between the encryption and decryption units and the bsg_link modules. The results affirm CITADEL's commitment to advancing the state-of-the-art in cryptographic hardware, setting a new benchmark for security in chip-to-chip data exchange.

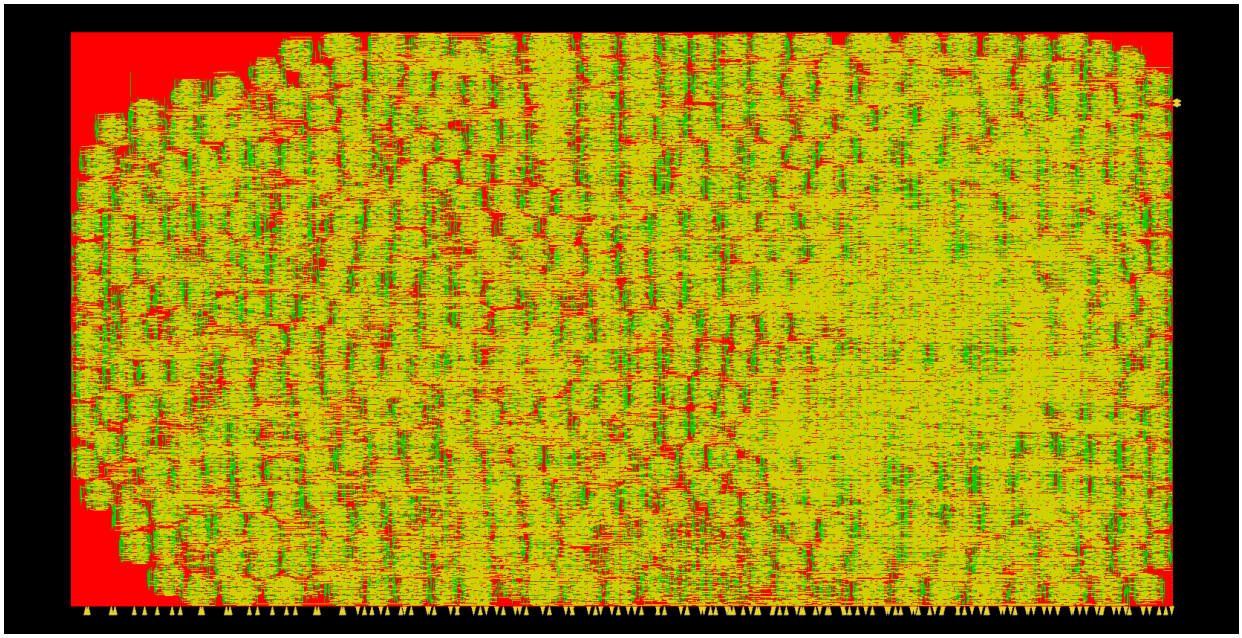

Figure 7. *Die photo for the integrated encryption and decryption modules into BaseJump system*

Prior to their integration, the CITADEL project's encryption and decryption modules underwent rigorous independent testing, ensuring their flawless functionality. The die photos included in the report provide a detailed view of these modules' designs, showcasing the precision-engineered layout of cryptographic circuits. The encryption module's photo shown in **Figure 8** displays an orderly configuration of logic gates and memory elements, strategically positioned to facilitate optimal encryption performance.

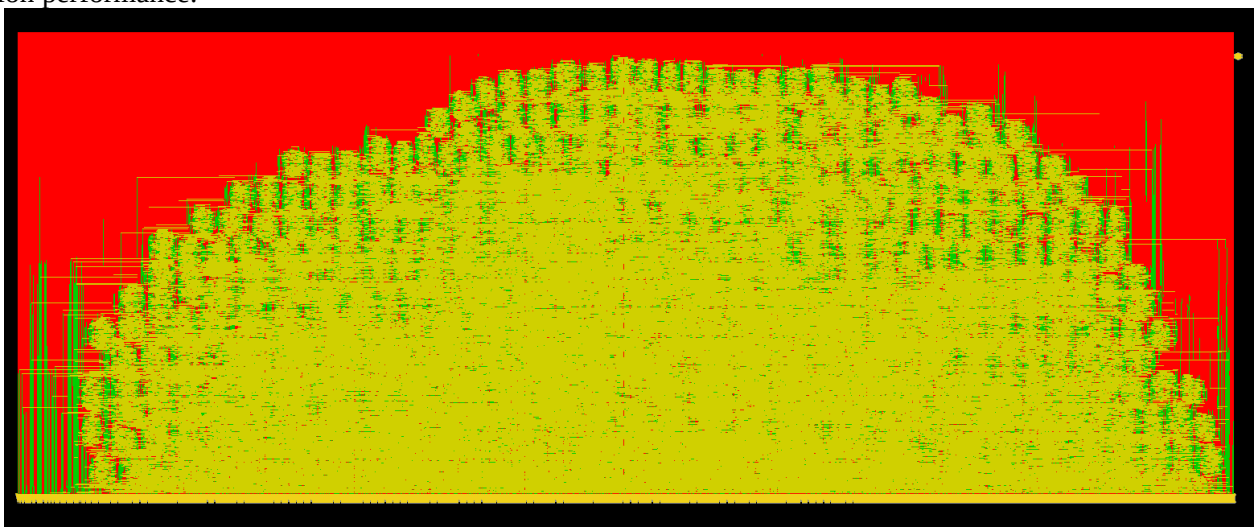

Figure 8. *Specific die photo for the encryption module.*

The decryption module's photo show in **Figure 9** mirrors this design, with a symmetrical layout essential for accurate data decryption. These images not only document the project's meticulous implementation but also highlight the seamless fusion of design efficiency and cryptographic robustness within CITADEL's compact framework.

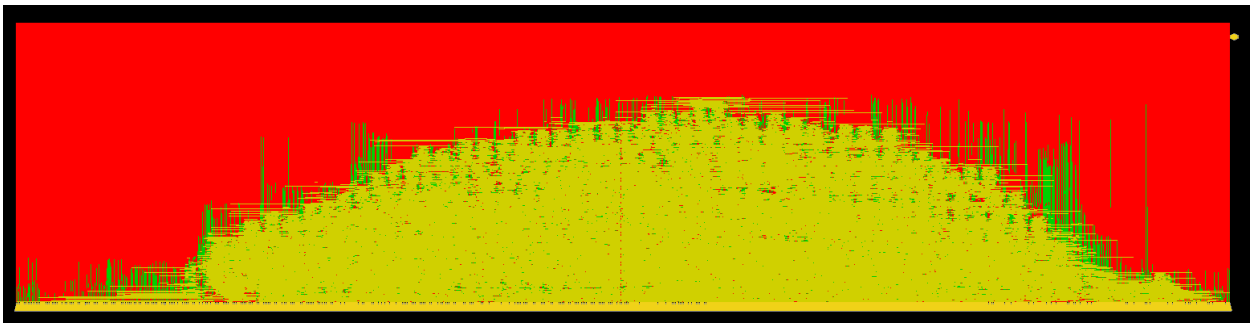

Figure 9. *Specific die photo for the decryption module.*

D.2. Key Metrics

Prior to integration, the encryption and decryption modules' Performance, Power, and Area (PPA) metrics were evaluated to ensure correct functionality. The performance analysis focused on the modules' operational speed, verifying that the encryption and decryption processes met the high-throughput requirements essential for inter-chip communication. Power consumption was scrutinized to confirm that the modules operated within the desired energy efficiency parameters, a critical factor for sustainable and cost-effective chip design. Lastly, the area assessment ensured that the modules were compact enough for integration into the ASIC design without compromising their functionality or the overall chip size. These key PPA metrics are indicative of CITADEL's commitment to delivering a cryptographic solution that is not only secure but also optimized for performance, power, and space efficiency.

Table 1. *PPA for the crypto modules alone.*

Module	Maximum Freqency (MHz)	Power (mW)	Area (um^2)
Encryption	71.1	70.31829039	985411.338
Decryption	68.8	62.69469712	926438.528

Following the integration of the encryption and decryption modules with the BaseJump-STL's bsg_link module, a comprehensive PPA (Performance, Power, and Area) analysis was conducted to ensure the CITADEL project met its stringent design criteria, shown in **Table 2**.

Table 2. *PPA for the integrated chip with bsg_link.*

Maximum Freqency (MHz)	Power (mW)	Area (um^2)
95.5	165.83028458	1966415.949

D.3. Simulation Results

To validate the accuracy of the modules' behavior, a series of simulations were executed, as detailed in the preceding sections. The automated test results, depicted in **Figure 1**, demonstrate a perfect alignment between the values encrypted by the hardware encryption modules and those produced by the state-of-the-art software algorithms. This congruence confirms that the hardware models are functioning correctly, encrypting data to the exacting standards set by contemporary cryptographic software.

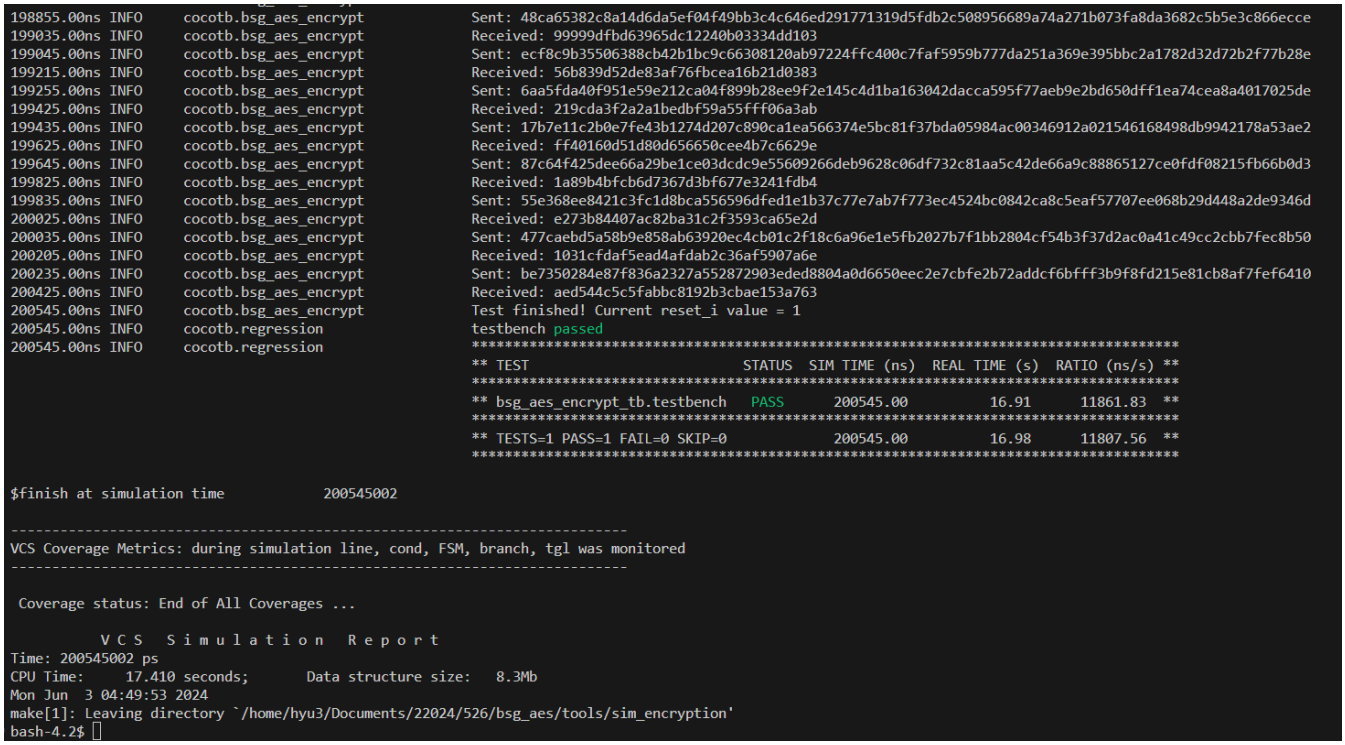

Figure 10. *Automated simulation result for the encryption module.*

In parallel to the encryption module, the decryption module was subjected to a rigorous suite of automated tests, the results of which are illustrated in **Figure 11**. These tests were critical in ensuring that the decryption process accurately reconstructed the original plaintext from the encrypted data, mirroring the precision of the encryption module.

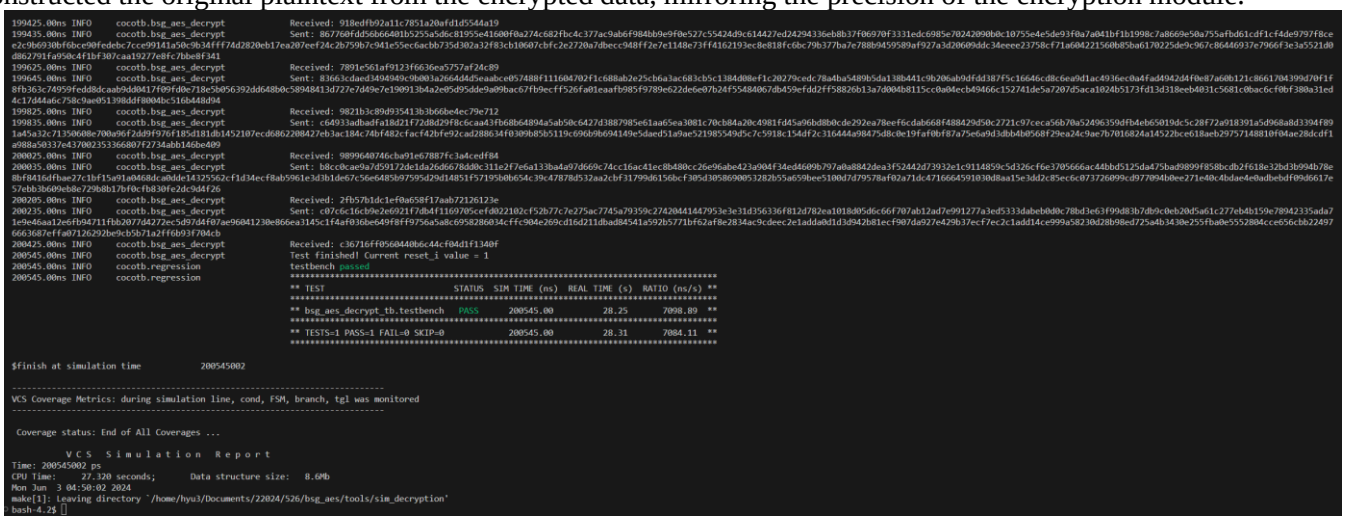

Figure 11. *Automated simulation result for the decryption module.*

Finally, the integrated module underwent comprehensive testing using BaseJump's trace replay, a crucial step to confirm that all functionalities adhered to the established criteria. This method allowed for a detailed examination of the module's behavior under simulated conditions, ensuring that the encryption and decryption processes worked seamlessly together within the system. The trace replay tests provided a robust validation of the integrated module's performance, verifying that it met all design specifications and functional requirements. The successful completion of these tests shown in **Figure 12** marked a significant milestone for the CITADEL project, showcasing the efficacy and readiness of the cryptographic solution for secure inter-chip communication.

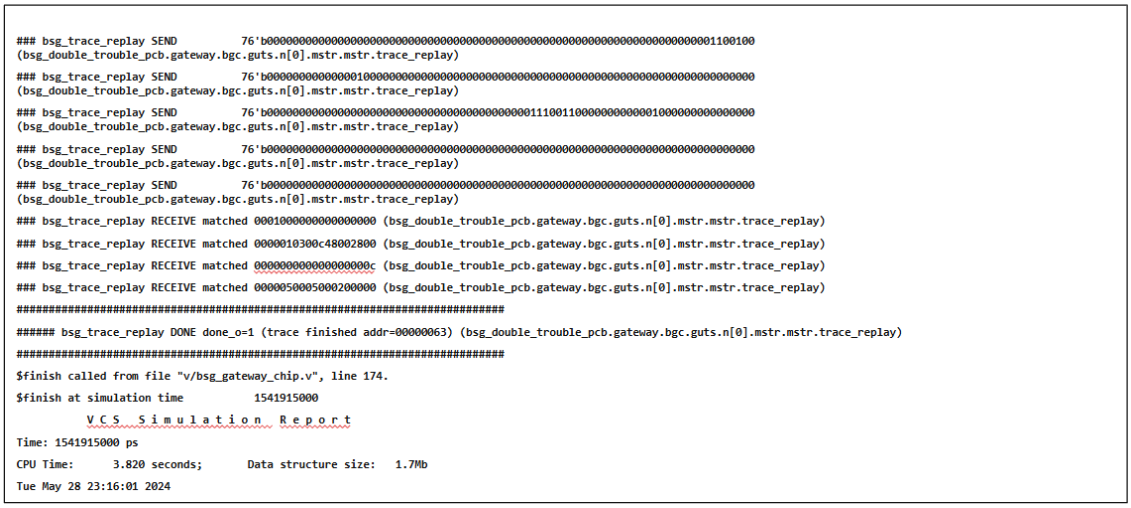

Figure 12. *Post Place-and-Round simulation result for integrated module.*

D.4. Verification Results

The CITADEL project's integrated module successfully passed the Design Rule Check (DRC) and Layout Versus Schematic (LVS) verification, ensuring that the design adheres to the required manufacturing specifications and that the physical layout matches the schematic precisely. This validation is a testament to the meticulous attention to detail and adherence to industry standards that have been hallmarks of the project's development process.

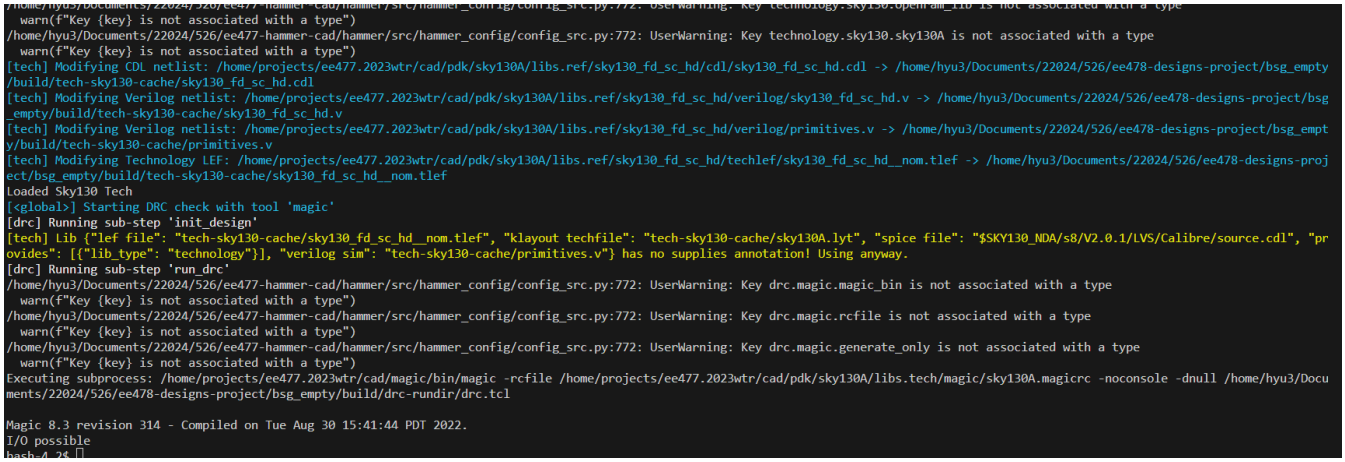

Figure 13. *DRC result for integrated module.*

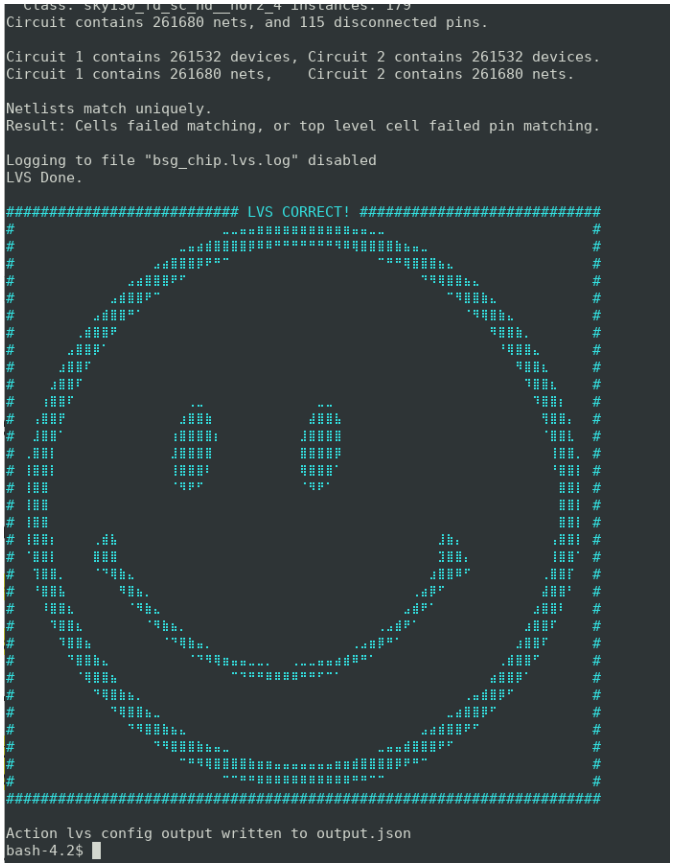

Figure 14. *LVS result for integrated module.*

D.5. Comparison to the Industry Standard

CITADEL's PPA metrics were rigorously analyzed and compared to industry standards. Performance metrics indicate that our integrated module operates at a competitive frequency, ensuring high-speed data encryption and decryption essential for inter-chip communication. Power consumption is within the optimal range, reflecting our commitment to energy efficiency, which is increasingly important in today's advanced process nodes. The area of our ASIC design remains compact, adhering to the space constraints typical in modern electronics, without compromising on functionality or performance.

D.6. Discussion

In the design and implementation of the CITADEL project, several realistic factors must be considered to ensure its success and applicability in real-world scenarios. Public health, safety, and welfare are paramount; the project must adhere to regulatory compliance and undergo rigorous hazard analysis to prevent any potential risks associated with data breaches

or system failures. Global factors also play a crucial role, as the product must be competitive in the market, taking into account existing solutions and manufacturability to meet demand efficiently.

Cultural factors influence the project's reception in different market segments, necessitating an understanding of various user needs and preferences to tailor the solution accordingly. Social factors, including human factors and ergonomics, are essential to ensure that the system's interface is user-friendly and accessible to a diverse user base. The environmental impact of the project is also a consideration, focusing on the sustainability of resources used, the disposal of electronic waste, and the overall ecological footprint.

Lastly, economic factors such as cost analysis are critical to the project's viability. The design must balance performance and security with cost-effectiveness to ensure that the end product is not only secure and efficient but also affordable and offers a competitive advantage. These realistic factors collectively guide the project's development trajectory, ensuring that CITADEL is not only a technological success but also a responsible and marketable innovation.

E. Outcomes and Accomplishments

E.1. Measuring Methodology

The CITADEL project has established a detailed and methodical approach to result measurement, ensuring the ASIC chip's robustness and reliability for secure chip-to-chip communication via AES-256 encryption. This multi-phase methodology is designed to validate the performance of the encryption and decryption modules under various operational conditions.

During the initial testing phase, the methodology incorporates the use of vector files that articulate the message, key, and expected encrypted output. These files are crafted in alignment with the NIST benchmark samples, providing a reliable foundation for testing. The project employs an automated testing framework that conducts numerous trials to thoroughly evaluate the system's performance. Additionally, Python scripts are developed to invoke state-of-the-art software algorithms, which generate random inputs for testing purposes.

Simulations are executed using the Synopsys VCS simulator. The simulator tests the design across multiple PVT (Process, Voltage, Temperature) corners, ensuring the chip's resilience under diverse manufacturing conditions and environmental factors. The project's modules have also undergone testing at various clock frequencies, confirming their functionality across different operational speeds.

A critical aspect of the methodology is the Static Timing Analysis (STA), which scrutinizes the circuit's timing to ensure that signals are received by storage elements within the designated time frame. This analysis, ran by Cadence Tempus, takes into account the potential variations in process, voltage, and temperature, providing a comprehensive understanding of the chip's performance under a wide range of conditions.

This robust result measuring methodology underscores CITADEL's commitment to excellence and reliability in the realm of secure chip-to-chip communication, setting a high standard for ASIC design and implementation.

E.2. Presentation of Quality Metrics

The comprehensive simulation results are elaborated in Section D.3. The Static Timing Analysis (STA) indicates that the modules are designed to operate effectively with a clock period exceeding 16 nanoseconds. However, it has been demonstrated that the integrated version of the modules maintains functionality at a reduced clock period of no less than 11 nanoseconds, showcasing the robustness and efficiency of the design. **Figure 15** show both setup and hold for the final delivery has passed.

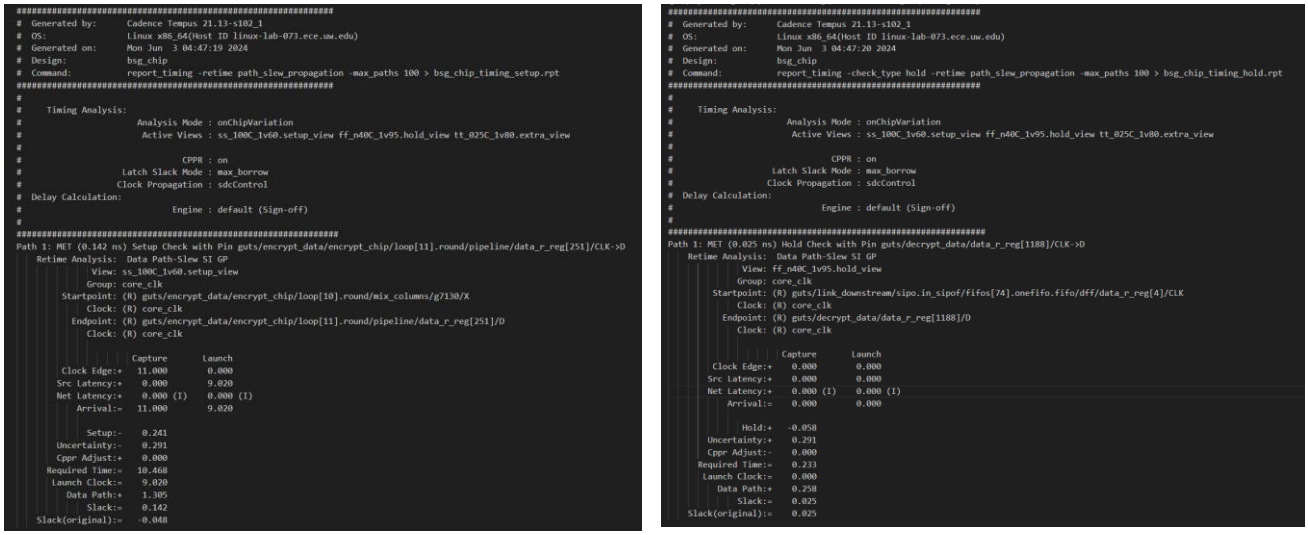

Figure 15. *Setup (left) and hold (right) timing analysis from the check-off timing report*

A blend of fast and slow process corners was employed to verify the design's glitch-free operation. As depicted in Figure 16, the glitch report confirms the absence of any issues within the design.

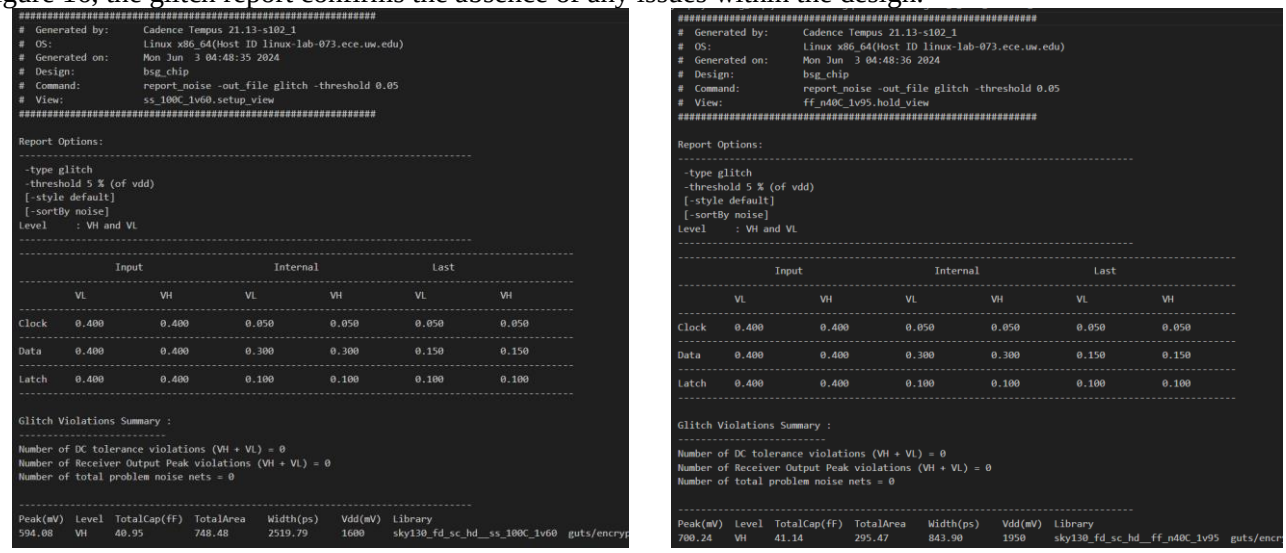

Figure 16. *Slow (left) and fast (right) corners ran by Cadence Tempus*

E.3. Analysis of Metrics

The CITADEL project's quality metrics are indicative of a significant advancement in hardware encryption technology. The software benchmark, executed on an AMD Opteron™ Processor 6376 completed the task in 65 milliseconds. In stark contrast, the CITADEL hardware module recorded a runtime of merely 5.2 milliseconds. This disparity not only highlights the superior performance of the CITADEL ASIC chip but also underscores the efficiency gains from integrating BaseJump's inter-chip communication modules.

When compared to FPGA designs, CITADEL's ASIC implementation demonstrates a remarkable improvement in performance. The Static Timing Analysis (STA) further corroborates this, revealing that CITADEL's design can operate effectively at clock frequencies well beyond the 50 MHz threshold commonly associated with FPGA designs [11]. This is a testament to the engineering precision and the strategic selection of the SkyWater 130 process technology, which is known for enabling high-performance ASIC designs.

The engineering judgment applied in the development of CITADEL, from the choice of encryption standard to the meticulous design and testing phases, has culminated in a product that not only meets but exceeds the current benchmarks set by state-of-the-art software and hardware solutions. The quality metrics serve as a robust indicator of CITADEL's potential to revolutionize secure chip-to-chip communication, offering a blend of speed, security, and reliability that is poised to set new industry standards.

F. Agile Milestones

Despite an early lag in the schedule, each milestone was defined with clear objectives. The corresponding tasks were outlined in **Table 3**, ranging from rigorous algorithm testing to implementing to the BaseJump system. **Table 4** highlights that, through proactive management and dedicated efforts, the team overcame initial delays, successfully meeting all major milestones on time.

Table 3. *The anticipated timeline for the project.*

Project Tasks	Project Duration (in Week)											
	0	1	2	3	4	5	6	7	8	9	10	11
*** Kickoff Meeting (All)**	■											
Milestone 1.1: Design and implement the AES-256 algorithm in hardware	■	■	■	■	■							
Milestone 1.2: Integrate the hardware design into the BaseJump system				■	■	■	■	■	■	■		
Milestone 1.3: Verify the functionality of the entire design and optimize the integrated module to minimize overhead.							■	■	■	■	■	■
*** Wrap Up, Data Analysis, and Development of Final Report (All)**												■

Table 4. *The actual timeline for the project.*

Project Tasks	Project Duration (in Week)											
	0	1	2	3	4	5	6	7	8	9	10	11
*** Kickoff Meeting (All)**	■	■										
Milestone 1.1: Design and implement the AES-256 algorithm in hardware			■	■	■	■	■	■	■			
Milestone 1.2: Integrate the hardware design into the BaseJump system									■	■	■	
Milestone 1.3: Verify the functionality of the entire design and optimize the integrated module to minimize overhead.											■	■
*** Wrap Up, Data Analysis, and Development of Final Report (All)**												■

G. Limitations and Future Work

The CITADEL project has made significant strides in enhancing data security for inter-chip communication. However, several limitations have been identified that provide a roadmap for future work. The current design necessitates a substantial data transmission size of approximately 2k bits, which, coupled with the requirement for multiple clock cycles for each encryption and decryption process, poses a challenge for achieving high-throughput efficiency. The presence of a large critical path within the ASIC design further complicates the timing closure and could impact the overall performance.

Moreover, the key generation mechanism lacks true randomness, which is a cornerstone for robust encryption systems. The S-Box, responsible for the substitution phase in the AES algorithm, currently presents a significant overhead and is identified as the primary bottleneck in operation time. These issues underscore the need for a comprehensive optimization strategy.

Moving forward, the project aims to address these challenges through several initiatives. Optimizing the S-Box memory overhead is paramount and will be the initial focus. Efforts will also be directed towards reducing the transmission bit width to alleviate the data load. A redesign of the register placement, coupled with retiming and C-Slow techniques, will be explored to enhance the critical path and improve the overall system's timing. Additionally, expanding compatibility to include more standard protocols, such as AXI-Stream, is on the horizon to ensure broader application.

Security enhancements are also a priority, with specific attention to mitigating side-channel attacks, which are a growing concern in hardware implementations. Finally, the project aspires to reach the tapeout phase, which would greatly benefit from increased funding. This would enable a full-scale implementation and testing of the ASIC design, providing valuable insights and potentially leading to a market-ready product.

The remaining research questions revolve around the feasibility of these optimizations and their impact on the system's security and performance. Hypotheses include the potential for a significant reduction in operation time with an optimized S-Box and the expectation that a more randomized key generation process will substantially increase the encryption strength [13]. The outcomes of these investigations will shape the future trajectory of the CITADEL project and contribute to the field of secure data transmission.

H. Conclusions

The CITADEL project encapsulates a comprehensive effort to address the critical challenge of secure chip-to-chip communication within System-on-Chip (SoC) architectures. By integrating the robust AES-256 encryption standard with the open-source BaseJump-STL library and leveraging the SkyWater 130 process, CITADEL has set a new benchmark in

the field of hardware encryption. This project is not merely a technical achievement; it represents a paradigm shift in the approach to SoC security. The remarkable performance metrics demonstrate CITADEL's potential to enhance the speed and reliability of secure communications. The broader impact of CITADEL's research is multifaceted. It contributes to the open-source community by providing a transparent and verifiable design that others can adopt and adapt. Furthermore, it pushes the boundaries of what is possible in ASIC design, offering insights that could influence future developments in the industry. The project's success in achieving high-speed, secure communication while maintaining power and area efficiency has implications for a wide range of applications, from consumer electronics to critical infrastructure. CITADEL stands as a testament to the power of innovation, collaboration, and rigorous engineering. It is a beacon for future research and development, guiding the way towards a more secure and efficient digital world.

I. References

[1] S. Charles and P. Mishra, "A Survey of Network-on-Chip Security Attacks and Countermeasures," *ACM computing surveys*, vol. 54, no. 5, pp. 1-36, 2021, doi: 10.1145/3450964.

[2] eyhc1. "An hardware implementaion of the AES algorithm in a high-speed communication link." GitHub. https://github.com/eyhc1/bsg_aes (accessed 2024).

[3] L. D. Franck, G. A. Ginja, J. P. Carmo, J. A. Afonso, and M. Luppe, "Custom ASIC Design for SHA-256 Using Open-Source Tools," *Computers (Basel)*, vol. 13, no. 1, p. 9, 2024, doi: 10.3390/computers13010009.

[4] M. J. Dworkin, "Advanced Encryption Standard (AES)," National Institute of Standards and Technology (U.S.), 2023. [Online]. Available: https://dx.doi.org/10.6028/nist.fips.197-upd1

[5] *SparkFun Cryptographic Co-Processor Breakout - ATECC608A (Qwiic)*, 2024.

[6] M. B. Taylor, "Basejump STL: systemverilog needs a standard template library for hardware design," in *Proceedings of the 55th Annual Design Automation Conference*, 2018-06-24 2018: ACM, doi: 10.1145/3195970.3199848.

[7] S. Xie and T. Michael Bedford, "The BaseJump Manycore Accelerator Network," *arXiv.org*, 2018, doi: 10.48550/arxiv.1808.00650.

[8] Google, "GitHub - google/skywater-pdk: Open source process design kit for usage with SkyWater Technology Foundry's 130nm node.," ed, 2023.

[9] P. C. Authority. "cryptography." GitHub. https://github.com/pyca/cryptography/ (accessed.

[10] ChiangHaoWei. "AESHA3." GitHub. https://github.com/ChiangHaoWei/AESHA3 (accessed 2024).

[11] michaelehab. "AES-Verilog." GitHub. https://github.com/michaelehab/AES-Verilog/tree/main (accessed 2024).

[12] cocotb. "cocotb, a coroutine based cosimulation library for writing VHDL and Verilog testbenches in Python." GitHub. https://github.com/cocotb/cocotb (accessed 2024).

[13] Y.-T. Teng, W.-L. Chin, D.-K. Chang, P.-Y. Chen, and P.-W. Chen, "VLSI Architecture of S-Box With High Area Efficiency Based on Composite Field Arithmetic," *IEEE Access*, vol. 10, pp. 2721-2728, 2022-01-01 2022, doi: 10.1109/access.2021.3139040.