Encryption Algorithm Benchmarking with the Nexys A7

Brad Bolluyt
ECE Department
Cal Poly Pomona
Pomona, California

Charles Tran
ECE Department
Cal Poly Pomona
Pomona, California

Elizabeth Woo
ECE Department
Cal Poly Pomona
Pomona, California

Steven Do
ECE Department
Cal Poly Pomona
Pomona, California

***Abstract*—This paper presents a comprehensive benchmark analysis of three widely used encryption algorithms, namely RSA, DES, and AES, implemented on the Nexys A7 FPGA platform. The study aims to provide insights into the performance characteristics and efficiency of these cryptographic techniques when deployed in a hardware environment. The Nexys A7 FPGA serves as the experimental platform for evaluating the encryption methods.**

The benchmarking process involves assessing the execution time and resource utilization of each encryption algorithm on the FPGA. Results reveal the strengths and weaknesses of RSA, DES, and AES when implemented on the Nexys A7 FPGA, shedding light on their respective trade-offs in terms of speed and efficiency. The findings presented in this paper aim to help decide most suitable encryption algorithm for applications requiring a balance between security and hardware resource constraints in FPGA-based systems.

I. Introduction

In the realm of secure communication and data protection, selecting an encryption algorithm is critical for ensuring the confidentiality and integrity of sensitive information. This paper addresses this need by presenting a benchmark analysis of three prominent encryption algorithms—RSA, DES, and AES—executed on the Nexys A7 field-programmable gate array (FPGA) platform.

The Xilinx Vivado Design Suite played a central role in synthesizing and analyzing these algorithms, providing detailed metrics on performance. To streamline our focus on algorithmic performance, tests and simulations were conducted using a bare-metal implementation approach. This choice eliminates additional layers introduced by operating systems, allowing a direct exploration of RSA, DES, and AES capabilities and limitations on the Nexys A7 FPGA.

The subsequent sections delve into our experimental setup, methodology, and benchmark results. This study aims to provide concise insights into the comparative performance of these algorithms on the Nexys A7 FPGA, assisting practitioners and researchers in informed decision-making for resource-constrained embedded systems.

II. Types of Algorithms

In cryptography, symmetric encryption uses a single shared key for both encryption and decryption, making it computationally efficient and suitable for encrypting large amounts of data. Asymmetric encryption, on the other hand, involves a pair of mathematically related keys—a public key for encryption and a private key for decryption. While asymmetric encryption is slower due to complex mathematical operations, it is commonly used for secure key exchange, digital signatures, and establishing secure communication channels. The choice between symmetric and asymmetric encryption depends on the specific requirements of the cryptographic application.

A. DES Algorithm

The Data Encryption Standard (DES) is a symmetric key encryption algorithm developed by IBM in the 1970s and later standardized by the U.S. National Institute of Standards and Technology (NIST) to secure electronic data [2]. Operating on fixed-size blocks, typically 64 bits, DES employs a single secret key for both encryption and decryption [2]. Its process involves substitution and permutation operations across multiple rounds to transform plaintext into ciphertext and vice versa [2]. Despite its historical importance, DES is considered a legacy algorithm due to its vulnerability to modern brute-force attacks [2]. More secure encryption standards, such as AES, have largely supplanted DES in contemporary cryptographic practices [2].

B. AES Algorithm

AES, standing for Advanced Encryption Standard, is a widely embraced symmetric encryption algorithm crafted to protect sensitive information [3]. Officially standardized by the National Institute of Standards and Technology (NIST) in 2001, AES functions on fixed-size data blocks with key sizes of 128, 192, or 256 bits [3]. Through a series of substitution, permutation, and mixing operations executed across multiple rounds, AES adeptly transforms plaintext into ciphertext. Recognized for its robustness and adaptability, AES plays a pivotal role in securing data across applications such as internet communications, file encryption, and safeguarding sensitive information in various computing scenarios [3]. Its enduring security is rooted in its resilience against known cryptographic attacks and widespread adoption across diverse industries [3].

C. RSA Algorithm

RSA, named after its inventors Rivest, Shamir, and Adleman, is a widely used encryption method for secure communication and digital signatures [1]. In RSA, two keys are

created—a public one for encrypting and a private one for decrypting [1]. The security of RSA relies on the complexity of factoring the product of two large prime numbers, which forms the basis of its strong encryption. When sending messages, users can use the recipient's public key for encryption, and only the recipient, with the corresponding private key, can decrypt the message [1]. Additionally, RSA allows for digital signatures, ensuring the authenticity and integrity of data [1]. The sender uses their private key to create a signature that anyone can verify using the sender's public key [1].

III. Implementation and Findings

The evaluation of all three algorithms commenced with a synthesis in Vivado, marking the initial stage of our testing process. Hardware implementations were successfully generated for both DES and AES, allowing for comprehensive data collection, including power consumption and temperature metrics. However, due to time constraints, a hardware implementation for RSA was not feasible within the scope of this study. Consequently, there is a limitation in the availability of additional data specific to power consumption and temperature for RSA. Despite this constraint, the comparative analysis of DES and AES benefits from a more extensive dataset, providing valuable insights into their performance characteristics beyond just encryption and decryption speeds.

A. DES Implementation and Findings

The DES implementation showcases efficiency with a low utilization of resources on the board. With the highest delay recorded at 6.831 nanoseconds, the maximum frequency is approximately 146.39 MHz. The hardware implementation maintains the same resource utilization as in the synthesis phase. In terms of power consumption, the DES implementation demonstrates a modest usage of 0.106 watts. While the DES algorithm is fairly lightweight, it uses more on board resources than the AES algorithm, but less power. They are fairly comparable yet the DES algorithm is sorely lacking in terms of ability to prevent brute-force attacks.

B. AES Implementation and Findings

In comparison to both the prior DES and RSA implementations, the AES implementation stands out for its remarkable lightweight design. Utilizing merely 2 Look-Up Tables (LUTs) and 7 Input/Output ports (IOs), the AES algorithm exhibits significant efficiency, particularly when contrasted with the resource demands of DES. The highest delay observed in this implementation is 5.361 nanoseconds, resulting in a commendable maximum frequency of approximately 186.53 MHz. Notably, the power consumption is modest at 4.512 watts, primarily stemming from the use of 7 I/O ports. This lightweight nature positions AES as an optimal choice for applications where resource constraints and power efficiency are paramount considerations.

C. RSA Implementation and Findings

The implementation of RSA is notably more resource-intensive compared to symmetric encryption algorithms in terms of Look-Up Tables (LUTs), Flip-Flops (FFs), and Digital Signal Processors (DSPs). The highest delay recorded in this implementation is 339.878 nanoseconds, resulting in a maximum achievable frequency of approximately 2.94 MHz. Despite its relatively lower performance compared to symmetric algorithms, it's crucial to recognize that RSA serves a distinct purpose in securing the exchange of encryption keys. As an asymmetric algorithm, RSA has different applications than symmetric counterparts like AES or DES. While RSA may not be the optimal choice for high-speed data encryption, its significance lies in its efficacy for key exchange and digital signatures, highlighting the varied and complementary roles of different encryption methods in cryptographic systems.

IV. Conclusion

This comprehensive analysis explores the performance and characteristics of RSA, DES, and AES implementations on the Nexys A7 FPGA platform using the Xilinx Vivado Design Suite. RSA, known for secure key exchange and digital signatures, exhibited resource intensity. In contrast, DES showcased energy efficiency with lower power consumption compared to AES. AES, noted for its lightweight design and resource efficiency, outperformed both DES and RSA in this regard. These findings highlight the nuanced trade-offs in selecting encryption algorithms, emphasizing the importance of considering resource utilization, power consumption, and efficiency for specific application requirements.

References

[1] E. Yevgeny, "The RSA Algorithm," University of Washington, Department of Mathematics, 2009.

[2] National Institute of Standards and Technology (NIST), "Data Encryption Standard," NIST Special Publication 958, pp. 250-253.

[3] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197.