2024 International Conference on Smart Systems for Electrical, Electronics, Communication and Computer Engineering (ICSSEECC) | 979-8-3503-7817-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSSEECC61126.2024.10649478

Resource Analysis of Lightweight Cryptography Algorithms for Compact Devices

BABU KARUPPIAH A
Department of ECE
Sri Eshwar College of Engineering, Coimbatore
Tamilnadu, India
babukaruppiah.a@sece.ac.in

RAJARAJA R
Department of ECE
PSG Institute of Technology and Applied Research
Tamilnadu, India
rajaraja@psgitech.ac.in

RESMA MADHU P K
Department of ECE
PSG Institute of Technology and Applied Research
Tamilnadu, India
resmamadhu@psgitech.ac.in

SUSITHRA N
Department of ECE
PSG Institute of Technology and Applied Research
Tamilnadu, India
susithra@psgitech.ac.in

PRADEEPIKA N
Department of ECE
PSG Institute of Technology and Applied Research
Tamilnadu, India
211134@psgitech.ac.in

GOPIKA G
Department of ECE
PSG Institute of Technology and Applied Research
Tamilnadu, India
211115@psgitech.ac.in

Abstract — **The increasing number of sensitive electronic transactions highlights the need for fast and secure communication networks. Cryptographic algorithms offer a means to securely transmit information over communication channels. As data rates rise, software-based encryption becomes inadequate. Hardware implementation of cryptographic algorithms and their associated keys provides greater physical security, as they are not easily accessed or altered by external users. Enhancing the reliability of the algorithms, as well as their speed performance and implementation flexibility, are key areas of focus. This study proposes to compare the resource utilization of lightweight cryptography algorithms, specifically LED and ZORRO. The ZORRO algorithm uses 128-bit block and key sizes and operates through 24 rounds, with each round consisting of four transforms, the last two being identical operations. These rounds enhance security and operational efficiency. Additionally, the LED algorithm, known for its compactness and versatility in providing various security services, is also examined. It is widely used in applications such as RFID, smart cards, and sensor networks. This research aims to analyse the resource utilization of these algorithms using Xilinx FPGA.**

Keywords— Cryptography, LED, Zorro, FPGA

I. INTRODUCTION

Cryptography is the practice of safeguarding secrets through the use of codes and ciphers, confirming that only the intended recipient and the sender can access the message content. The term derives from the Greek words "crypt," meaning "hidden," and "graphy," meaning "writing." One of the earliest ciphers, the "Caesar cipher," was created by Julius Caesar around 100 BC for sending confidential messages. Caesar encoded his messages by shifting each letter three places to the right, making them appear random and meaningless to interceptors. Approximately four thousand years ago, the Egyptians used a form of cryptography known as "hieroglyphs." Scribes employed these secret codes to convey messages for the pharaohs. In modern cryptography, techniques to protect information are based on mathematical concepts and algorithmic rules. These algorithms are crucial for digital signatures, secure web browsing, and safeguarding online transactions such as credit card payments.

Today, cryptography is widely used to secure digital information, transforming data into an unreadable format that unauthorized users cannot access. The data remains indecipherable until decrypted with the correct key. Cryptography is integrated into daily life through computer passwords, ATM security, and personal emails, providing both information protection and user authentication. Cryptography involves both encryptions, which is the method of arriving at the cipher text by converting the plaintext into it, and cryptanalysis, which is the study of breaking codes. Key terms include:

Plaintext: The original readable information.

Cipher text: The altered, unreadable message intended for recipients.

Key: The sequence that controls the cryptographic algorithm's operation.

Encryption: The methods adopted to transform plaintext into cipher text.

Decryption: The method of getting back the plaintext from the cipher text

1.1 Types of Cryptography

Cryptography can be broadly classified into three main categories: symmetric key cryptography, asymmetric key cryptography, and hash functions.

Symmetric Key Cryptography:

Also given a name as secret key cryptography, symmetric key cryptography uses the same key for both the encryption and decryption processes, making it a conventional method of encryption. The security of this approach lies in directly dependent on the key used. It can be applied to both data in transit and data at rest. Symmetric cryptography is further subdivided into:

- Stream cipher
- Block cipher

SYNTHESIS RESULT OF ZORRO:

In ZORRO encryption the number of Slices used is 321. The utilized numbers of slice flip flops and 4 input LUTS are 71 and 609 respectively.

Logic utilization (in number)	Used	Available	Utilization
Slices	321	4656	6%
Slices Flip Flops	71	9312	0%
4 input LUTS	609	9312	6%
Bonded IOBS	257	66	389%
GCLKs	1	24	4%

TABLE V. DEVICE UTILIZATION REPORT OF ZORRO ENCRYPTION

.

The ZORRO algorithm demonstrates outstanding efficiency in resource utilization compared to the LED algorithm. Specifically, the Zorro algorithm uses only 321 slices, significantly fewer than Zorro's 517 slices. It also requires just 71 slice flip-flops, whereas LED needs 138. In terms of 4-input LUTs, the Zorro algorithm employs 609, while LED uses 955, indicating a more optimized approach by Zorro. Notably, both algorithms utilize the same number of bonded IOBs, which is 257, and a single global clock. This substantial difference in resource usage highlights the Zorro algorithm's superior efficiency, making it an excellent choice for applications on Xilinx FPGAs that prioritize minimal resource consumption.

IV. CONCLUSION AND FUTURE WORK

This research focuses on the encryption implementations of the block ciphers LED and ZORRO. The iterative architecture is purposefully crafted to minimize area utilization. Both encryption processes were effectively simulated using the ISIM simulator and synthesized utilizing the XST synthesizer on the Spartan 3E device. The results show that the Zorro implementation uses significantly fewer resources than the LED implementation, occupying only 321 slices, 71 flip-flops, and 609 four-input LUTs. In contrast, LED requires 517 slices, 138 flip-flops, and 955 four-input LUTs. The primary aim of this work is to analyze the area utilization of the LED and ZORRO algorithms, demonstrating that Zorro is more efficient in this regard. Other factors such as power consumption and security improvements are not considered in this study but could be topics for future research. Further efforts could focus on reducing power consumption and enhancing security features.

REFERENCES

[1]. Lightweight Cryptography Working Group. Cryptrec Cryptographic Technology Guideline (Lightweight Cryptography), March 2017.

[2]. Eisenbarth, Thomas, et al. "Compact implementation and performance evaluation of block ciphers in ATtiny devices." International Conference on Cryptology in Africa. Springer, Berlin, Heidelberg, 2012.

[3]. Borghoff, Julia, et al. "PRINCE–a low-latency block cipher for pervasive computing applications." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2012.\

[4]. Posteuca, Raluca, Cristina-Loredana Duta, and Gabriel Negara. "New approaches for round-reduced PRINCE cipher cryptanalysis."Proceeding of the Romanian A- mathematics physics technical sciences information science 16 (2015): 253-264.

[5]. Shahverdi, Aria, Cong Chen, and Thomas Eisenbarth. "AVRprince-an efficient implementation of PRINCE for 8-bit microprocessors." Technical report, Worcester.

[6]. K. P. Singh, and S. Dod. "An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm," IACR Cryptology ePrint Archive 2016 (2016): 789.

[7]. U. Farooq and M. F. Aslam. "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA," Journal of King Saud University-Computer and Information Sciences, vol. 29, pp. 295-302, 2017.

[8]. H. Mestiri, F. Kahri, B. Bouallegue, and M. Machhout. "A high-speed AES design resistant to fault injection attacks," Microprocessors and Microsystems 41, pp. 47-55, 2016.

[9]. P. Katkade, and G. M. Phade. "Application of AES algorithm for data security in serial communication," In 2016 International Conference on Inventive Computation Technologies (ICICT), vol. 3, pp. 1-5. IEEE, 2016.

[10]. M. Bedoui, H. Mestiri, B. Bouallegue, and M. Machhout. "A reliable fault detection scheme for the AES hardware implementation," In 2016 International Symposium on Signal, Image, Video and Communications (ISIVC).

[11]. T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, “A survey of lightweight-cryptography implementations,” IEEE Design & Test of Computers, vol. 24, no. 6, pp. 522–533, 2007.

[12]. G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, “A review of lightweight block ciphers,” J. Cryptograph. Eng., vol. 8, no. 2, pp. 141– 184, 2017.

[13]. M. Liskov, R. L. Rivest, and D. Wagner, “Tweakable block ciphers,” J. Cryptology, vol. 24, no. 3, pp. 588– 613, 2010.

[14]. L. Martin, “XTS: A mode of AES for encrypting hard disks,” IEEE Security & Privacy Magazine, vol. 8, no. 3, pp. 68–69, 2010.

[15]. M. Henson and S. Taylor, “Memory encryption: A survey of existing techniques,” ACM Computing Surveys, vol. 46, no. 4, pp. 1–26, 2014.

[16]. S. Ali, X. Guo, R. Karri, and D. Mukhopadhyay, “Fault attacks on AES and their countermeasures,” in Proc. Secure System Design Trustable Computing, 2016, pp. 163– 208.IEEE, 2016.

[17]. L. R. Knudsen, “Iterative Characteristics of DES and s2-DES,” Advances in Cryptology: Proceedings of CRYPTO ’92, pp. 497–511, 1992.

[18]. D. Coppersmith, “The Data Encryption Standard (DES) and its Strength Against Attacks,” IBM Journal of Research and Development, IBM Thomas J. Watson Research Center, Technical Report RC 186131994, December 1994.

[19]. D. Davies and S. Murphy, “Pairs and Triplets of DES S-Boxes,” Journal of Cryptology, vol. 8, no. 1, pp. 1– 25, 1995.

[20]. D. Dinu, J. Großschädl, Z. Liu, and T. Wenger, "Lightweight Cryptography for IoT: Energy-Efficient Implementation of Led and LED64 on MSP430 Microcontroller," IEEE Transactions on Computers, vol. 70, no. 3, pp. 341-352, March 2021, doi: 10.1109/TC.2020.3008151.

[21]. S. A. Seyedzadeh, S. Hashemi, and R. C. C. Cheung, "Efficient FPGA Implementation of Lightweight Block Cipher LED Using Composite Field Arithmetic," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 6, pp. 1168-1172, June 2021, doi: 10.1109/TVLSI.2021.3069754.

[22]. A. Biryukov and I. Nikolić, "Cryptanalysis of the Zorro Lightweight Block Cipher," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3167-3177, December 2021, doi: 10.1109/TIFS.2021.3072236.

[23]. T. Beyne, Q. Meunier, and F. Standaert, "Improved Analysis of the Zorro Lightweight Block Cipher," IEEE Transactions on Information Theory, vol. 67, no. 4, pp. 2768-2782, April 2021, doi: 10.1109/TIT.2021.3054018.