Data Analytics and Artificial Intelligence
Vol: 2(5), 2022
REST Publisher; ISBN: 978-81-948459-4-2
Website: http://restpublisher.com/book-series/data-analytics-and-artificial-intelligence/

Advanced Encryption Standard algorithm in Cyber Security

* **Archana B U, V Niranjana**
REST Labs, Kaveripattinam, Krishnagiri, Tamil Nadu, India.
*Corresponding author Email: archanabu3129@gmail.com

Abstract. Because of the broad range of distant exchanges of information, the encryption process has become a crucial component for almost every data transaction application. Every day, a massive amount of sensitive data is transferred. Through various channels such as e-commerce, electronic banking, and even simple email applications The Advanced Encryption Standard (AES) algorithm has been used as the most effective option for various security services in a wide range of applications. As a result, many studies are focusing on that algorithm to improve its efficiency and performance.This paper provides an overview of slashing research for AES algorithm issues and aspects in terms of development, implementation, and evaluation. This paper's involvement is aimed at laying the groundwork for future AES algorithm development and implementation. It also opens the way to using techniques for machine learning to enact the AES algorithm.
Keywords: Cryptography Advanced Encryption Standard, Machine Learning.

1. Introduction

Cryptography is the process of converting data into a jumbled layout while also permitting a receiver to recover the actual information using a private key. The two primary functions of any cryptography system are encryption and decryption. Encryption is the method of transforming data into an unintelligible format and use a secret key to ensure the user's privacy. Decryption is the opposite function that uses a private key to retrieve the original encrypted information. Data encryption is a critical step in nearly all data transaction applications [1]. Encrypting data algorithms are categorized into two categories: symmetric key and asymmetric key [2]. Communication is accomplished only using one key in synchronous or secret key algorithms. Asymmetric key algorithms, on the other hand, use more than one key for data encryption and restoration. One key is a public key.The first key is a public key that is used for data encryption, while the second key is a secret key that is used for data decryption. Symmetric algorithms are much faster than asymmetric key algorithms, which require a larger key and more complex computation [1], [3]. The Advanced Encryption Standard (AES) [4] algorithm is a symmetric key block cipher whose block size ranges from 64 to 256 bits as processors become more sophisticated. Although the AES can accept blocks of 128 or 256 bits in size, it remains a large slow when compared to stream-based ciphers at a time when all applications, including such web applications and ATMs, require faster encryption (ATMs). Some AES applications, on the other hand, continue to struggle for low implementation areas, such as smart card and cellular phone-related hardware. As a result, the encryption speed and implementation area are two critical factors in the real-time deployment of the AES algorithm. The issue with AES spreading is the compromise between encryption and decryption.The contribution of this research is to report on state-of-the-art implementations of the AES algorithm on FPGA modules, with a focus on the raised implementation issues and aspects. This contribution is significant for future AES encryption algorithm advancements and implementations. It is used as a baseline for evaluating any new AES developments by comparing the output results of the proposed approaches to the results reported in this study. The remainder of this paper is structured as follows. Section 2 provides a theoretical foundation for the AES algorithm in terms of algorithm structure, data encryption, and data decryption methodologies. Section 3 presents cutting-edge research on AES implementation in an FPGA environment with speed and area constraints. Section 3 also contains information about the new machine-learning implementation of AES. Section 4 reports the findings and upcoming projects.

2. Advanced Encryption Standard Algorithm

The Data Encryption Standard (DES) [9] has been used as a framework for symmetric key cryptography with a key length of 56 bits. However, the key length has shrunk and is easily hacked [10]. The encryption operation is carried out on a two-dimensional array of bytes called State (each block is organized as a 4 4 matrix of bytes), which comprises four rows of Nb bytes each. Consider the AES 128 algorithm, whose initial round state is XOR with a chosen key. Sub Bytes, Shift Rows, Mix Columns, and Add Round Key are the 4 major processes in a regular round. Only three operations are found in the final round, while the Mix Columns operation is eliminated [15]. In present-day cryptography, AES is widely adopted and supported in both hardware and software. To date, no practical cryptanalytic attacks against AES have been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches. However, just as for DES, AES security is assured only if it is correctly implemented and good key management is employed.

3. How Does AES Encryption Work?

For transmissions from the sender to the receiver and from the receiver to the sender, there is only one key. This key is used by AES to encrypt and decode data via a mathematical process. The AES encryption method is widely renowned for its speed and security. The security of the algorithm comes from the data being encrypted using a complex block cipher technique. And AES uses less processing power so it is faster than other equivalents AES, like many other block ciphers, performs cipher transformations using rounds of encryption. It divides the input plaintext into a four-row, four-column block. Each box contains one byte, with a total of 16 bytes in a block. Each round is made up of various building steps that work together to form a function that is then repeated multiple times. The number of rounds performed by AES is determined by the length of the key. It does 10 rounds at 128 bits, 12 rounds at 192 bits, and 14 rounds at 256 bits. With the algorithm running in each round, a previous state and a Round key are created at the end. According to FIPS 197, the Round Key is produced from the cryptographic key using the Rijndael key schedule. After the last AES cycle, the State produces "cipher text", which has no relation to plaintext. In the inverse of the encryption processes, decryption of the cipher text is performed using the same symmetric key used for encryption. AES is built on a substitution-permutation network, in which the input field(commonly known as "plaintext") and the cryptographic key are processed in a series of mathematical operations using substitution boxes (S-boxes) or permutation boxes (P-boxes). There are mainly 4 operations while converting the plaintext data into cipher text through the use of a secret key.

Sub Bytes: SubBytes transformation is the initial stage of each round. This stage relies on a nonlinear S-box to replace a byte in the state with a different byte. For example, if the hexadecimal code for a byte was 84, the procedure would be to identify the cell in the S-box where row 8 and column 4 intersect, and that value would be used. According to the graphic below, the new value in this scenario would be "5f".

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 1. S-Box: Substitution values for the byte XY (hexadecimal format)

Shift Row: To produce diffusion, the data is shifted from its initial location. The goal of Shift Rows is to relocate the data locations in their appropriate rows using wrapping. The first row is left unchanged. With the row wrapped around, the second row pushes the bytes to the left by one place. With the row wrap around, the third row pushes the bytes to the left by two positions, and the fourth row shifts the bytes to the left by three positions.

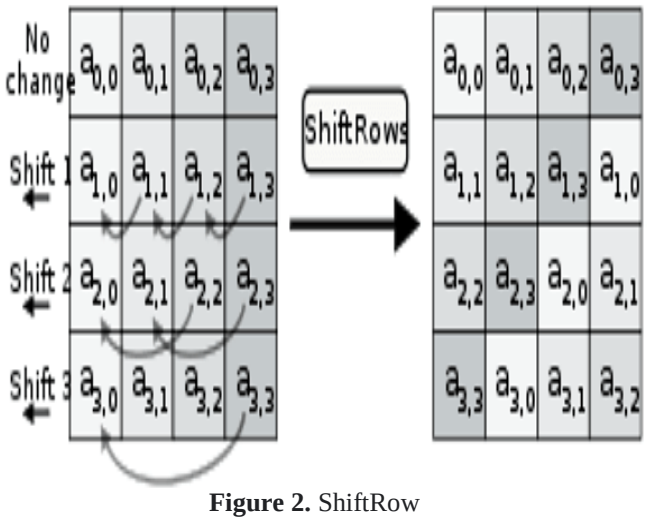

Figure 2. ShiftRow

Mix Column: In this step, the AES algorithm uses a mathematical process known as a linear transformation to combine the bytes. it performs a complicated XOR algorithm function on each column, combining all four-byte values mathematically and producing four new bytes as outputs.

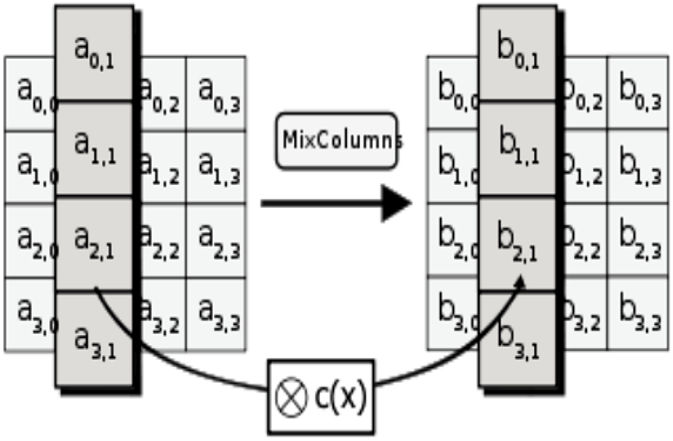

Figure 3. Mix Column

Add Round Key: This is the first and last operation that the state array goes through during encryption. It is the most vital stage in the algorithm. Each round generates a new key using a key schedule specific to the Rijndael algorithm on which the AES is based. The mixed column's result is added to the first round key. It then returns to the first step (Sub Byte) and the entire process (round) begins all over again.

4. What are the features of AES?

NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192, and 256 bits. Other criteria for being chosen as the next AES algorithm included the following:

Security: Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition. Cost: Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency. Implementation: Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

5. Benefits

The following are the benefits or advantages of AES:

- The encryption processes of AES are easy to learn, making it more attractive to those dealing with AES.
- It's easy to implement.
- Faster encryption and decryption times.
- AES consumes less memory and system resources.
- AES can be combined with other security protocols when it needs an extra security layer.
- As it is implemented in both hardware and software, it is the most robust security protocol.
- It uses higher length key sizes such as 128, 192, and 256 bits for encryption. Hence it makes the AES algorithm more robust against hacking.
- It is the most common security protocol used for a wide variety of applications such as wireless communication, financial transactions, e-business, encrypted data storage, etc.
- It is one of the most spread commercial and open-source solutions used all over the world.
- No one can hack your personal information.

For 128-bit, about 2^{128} attempts are needed to break. This makes it very difficult to hack it as a result it is a very safe protocol.

6. Conclusion

Data encryption is a fundamental concept in information security that is used by nearly all data transaction applications. The Advanced Encryption Standard (AES) is a highly efficient encryption algorithm that has been widely adopted. Because of its simplification and applicability, it has received a lot of research attention. AES-related research focuses on encryption speed and hardware implementation as two important factors in algorithm performance. This paper presented some cutting-edge studies for improving AES speed and implementation. According to the reported results, there is a clear trade-off between the two factors. We intend to continue this research in the future to achieve the fastest encryption speed in a limited implementation area. Acknowledgment: I am delighted to express my heartfelt appreciation to our department's head and staff, as well as family and friends. This paper is made possible by their encouragement, assistance, and support

Reference

[1]. van Tilborg, H.C.A.: Encyclopedia of Cryptography and Security. Springer-Verlag New York, Inc., Secaucus (2005).

[2]. Nedjah, N., de Macedo Mourelle, L.: A Versatile Pipelined Hardware Implementation for Encryption and Decryption Using Advanced Encryption Standard. In: Dayd´e, M., Palma, J.M.L.M., Coutinho, ´ A.L.G.A., Pacitti, E., Lopes, J.C. (eds.) VECPAR 2006. LNCS, vol. 4395, pp. 249–259. Springer, Heidelberg (2007).

[3]. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners, 1st and. Springer Publishing Company, Incorporated (2009).

[4]. Burr, W.E.: Selecting the advanced encryption standard. IEEE Security and Privacy1 (2), 43–52 (2003).

[5]. Kilts, S.: Advanced FPGA Design: Architecture, Implementation, and Optimization Wiley-IEEE Press (2007).

[6]. Gomes, O., Moreno, R., Pimenta, T.: A fast cryptography pipelined hardware developed in FPGA with VHDL. In: The 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp. 1–6 (October 2011).

[7]. Mijalli, M.H.A.: Efficient realization of S-Box based reduced residue of prime numbers using Virtex-5 and Virtex-6 FPGAs. American Journal of Applied Sciences 8(8), 754–757 (2011).

[8]. Dileep, A., Sekhar, C.: Identification of block ciphers using support vector machines. In: International Joint Conference on Neural Networks, IJCNN 2006, pp. 2696–2701 (2006).

[9]. National Institute of Standards and Technology: FIPS PUB 46-3: Data Encryption Standard (DES) (October 1999), http://www.itl.nist.gov/fipspubs/fip186-2.pdf supersedes FIPS 46-2.

[10]. Hoang, T., Nguyen, V.L.: An efficient FPGA implementation of the advanced encryption standard algorithm. In: IEEE RIVF International Conference on Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF), pp. 1–4 (March 2012).

[11]. National Institute of Standards and Technology, http://www.nist.gov/index.html.