Review of Advance Encryption Standard in Different Aspect

Poonam Shrivastava[1] Dr. Paresh Rawat[2]
[1]M. Tech Scholar [2]Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]Sagar Institute of Science and Technology, Bhopal (M.P.), India

Abstract— Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm. During the recent times, with the tremendous growth of digital data communication over computer network, information content security becomes a prime concern. Internet itself allows many security threats and those can easily corrupt the transferred data over network. The AES algorithm provides higher security with higher encryption speed and throughput but still modifications are going on to improve its performance. In this paper we survey on AES encryption techniques on different parameters and different platform for various applications.

Keywords: Cryptography, AES, Decryption, Encryption, Digital, Key

I. Introduction

The rapid growth of digital data transmission has significantly increased the importance of information security in our modern digital life. In data communication the development of new transmission technologies have ascended the need of specific strategy for security mechanisms. Network security has become more and more pivotal as digitalization and transmission of large data over internet have been transforming from time to time. Cryptography and different encryption techniques provide security and protection to the data transmitted over non secure networks used for digital transmission of data. The Advanced Encryption Standard (AES) known as Rijndael is a well-known symmetric block cipher algorithm adopted by the United States of America government as a national encryption algorithm and it provides portability, robustness and high level security against many cryptographic attacks. To have better performance, certain efforts have already been made in redesigning and reconstructing the AES algorithm. In this paper we are discussing about different modifications on AES algorithm and comparing their result on the basis of different parameters. To enhance the efficiency of AES, researchers sometimes modified the existing structure of the AES algorithm and sometimes merging the AES block cipher with other models from various fields. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. Cryptography plays an important role by providing security for digital transmission of data over such insecure network. Cryptographic protocols scramble data into unreadable text which can be only read or decrypted by those possesses the associated key.

Today it is widely acknowledged that security issues which are already of highest priority will continue to play a central role in the design of future IT systems. The range and areas of applications with security needs appear to be almost endless: Internet communications; constrained wireless devices (e.g., cell phones and wireless LAN), communication between cars, e-commerce, e-Banking, copy right protection of digital media (e.g., music and videos), electronic bar codes on consumer products (RFID), electronic stamps, etc.[1-6]. Therefore, design and implementations of security solutions in future will increasingly be quite a challenging undertaking since an attacker will attempt to attack the weakest link in the security systems. This could be via many available options, e.g. breaking the underlying crypto-algorithm and which in most cases is harder option to be attempted only as a last resort. Instead the eavesdropper might opt to exploit other weaknesses such as: recovering a key by observing the power consumption or electromagnetic radiation of the crypto-devices; finding vulnerabilities in the security protocols or simply revert to stealing the key: through clever interactive social engineering with those trusted to safeguard the keys. In most cases, however, the crypto-algorithms are always the most important core tool in security applications. Hence, the cryptographic algorithms have to be carefully designed, selected and implemented in order to avoid the core cryptography becoming the weakest link in any security solution.

Modern crypto-techniques are mathematical transformations (algorithms), which treat messages as numbers or algebraic elements in a space and transform them between a region of meaningful messages or cleartext and a region of unintelligible messages or ciphertext. In order to restore information, an encryption transformation must be reversible and the reversing transformation is called decryption. Conventional, encryption and decryption algorithms are parameterized by cryptographic keys. An encryption algorithm and a decryption algorithm plus the description on the format of messages and keys, form a cryptographic systems or a cryptosystem.

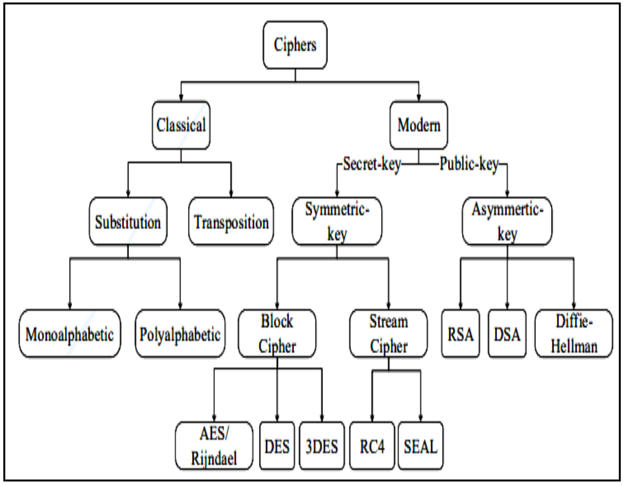

Fig. 1: Classification of Cryptographic Techniques [13]

II. LITERATURE SURVEY

R. Paul [1] Internet protocol security (IPSec), secure sockets layer (SSL)/transport layer security (TLS) and other security protocols necessitate high throughput hardware implementation of cryptographic functions. In recent literature, cryptographic functions implemented in software, application specific integrated circuit (ASIC) and field programmable gate array (FPGA). They are not necessarily optimized for throughput. Due to the various side-channel based attacks on cache and memory, and various malware based exfiltration of security keys and other sensitive information, cryptographic enclave processors are implemented which isolates the cryptographically sensitive information like keys. We propose a partitioned enclave architecture targeting IPSec, TLS and SSL where the partitioned area ensures that the processor data-path is completely isolated from the secret-key memory. The security processor consists of a Trivium random number generator, Rivest–Shamir–Adleman (RSA), advanced encryption standard (AES) and KECCAK cryptos. We implement three different optimized KECCAK architectures. The processing element (PE) handles all communication interfaces, data paths, and control hazards of network security processor.

R. Lumbiarres[2] This work presents a new hardware architecture designed for protecting the key of cryptographic algorithms against attacks by side-channel analysis (SCA). Unlike previous approaches already published, the fortress of the proposed architecture is based on revealing a false key. Such a false key is obtained when the leakage information, related to either the power consumption or the electromagnetic radiation (EM) emitted by the hardware device, is analysed by means of a classical statistical method. In fact, the trace of power consumption (or the EM) does not reveal any significant sign of protection in its behaviour or shape. Experimental results were obtained by using a Virtex 5 FPGA, on which a 128-bit version of the standard AES encryption algorithm was implemented.

D. Bui[3] Connected devices are getting attention because of the lack of security mechanisms in current Internet-of-Thing (IoT) products. The security can be enhanced by using standardized and proven-secure block ciphers as advanced encryption standard (AES) for data encryption and authentication. However, these security functions take a large amount of processing power and power/energy consumption. In this work, we present our hardware optimization strategies for AES for high-speed ultralow-power ultralow-energy IoT applications with multiple levels of security. Our design supports multiple security levels through different key sizes, power and energy optimization for both datapath and key expansion.

S. Shivkumar[4] The growing popularity of mobile and hand held devices ignited the growth of wireless networks over the past years. Wireless data communications have transformed not only the business world but also the human society by improving efficiency, flexibility, convenience, and above all productivity. Wireless Local Area Networks (WLAN) typically emulate the wired networks traditional hub-spoke configuration. The best known and most widely used variation of the 802.11 WLAN standard is 802.11b. Encryption in 802.11b is provided by Wired Equivalent Privacy (WEP), which has many weaknesses and flaws. Therefore the IEEE ratified 802.11i WLAN security standard in June 2004. The new cryptography was based on the Advanced Encryption Standard (AES) algorithm. The Substitution box (S-box) in AES brings non linearity to cryptosystem and strengthens their cryptographic security.

I. Hammad[5] This letter presents a new efficient architecture for high-speed advanced encryption standard (AES) encryption. This technique is implemented using composite field arithmetic byte substitution, where higher efficiency is achieved by merging and location rearrangement of different operations required in the steps of encryption. The proposed architecture is presented with multistage sub pipelined architecture that allows having higher efficiency in terms of (throughput/area) than any previous field-programmable gate array (FPGA) implementations.

Yulin Zhang[6] This work presents the outer-round only pipelined architecture for a FPGA implementation of the AES-128 encryption processor. The proposed design uses the Block RAM storing the S-box values and exploits two kinds of Block RAM. By combining the operations in a single round, we can reduce the critical delay. Therefore, our design can achieve a throughput of 34.7 Gbps at 271.15 Mhz and 2389 CLB Slices with 200 BRAM. We can get the much higher efficiency than any other implementation reported in the literature.

Z. Wang[7] Security issues emerged in recent years as the fast development of wireless technology, especially for mobile devices where computing resources are sparse. This work presents the implementation of RC4 as well as AES (Advanced Encryption Standard) cipher algorithm, which are widely used in IEEE 802.11 as well as IEEE 802.16 and other standards. The implementations target a novel reconfigurable instruction cell array (RICA) based architecture which has recently been developed, with the aim of achieving low power, high performance and programming flexibility. As our simulation result shows RC4 stream cipher throughput achieves as high as 60 Mbps with 128 bits key size and 1024 bits data buffer packet.

Table 2.1: Summery of Literature Survey

Sr.No.	Author Name	Publish Detail	Proposed Work	Remark
1	R. Paul	IEEE, 2018	Three different optimized KECCAK architectures based on AES and RSA	Throughput 39.98Gbps Clock 6 Clock frequency 234.97 MHz
2	R. Lumbiarres	IEEE, 2018	Proposed 128 bit AES	Performed on Virtex 5 FPGA, on which a 128-bit version
3	D. Bui	IEEE, 2017	Proposed lightweight	Implement 1 pJ/b at 10 MHz at 0.6 V

			standardized algorithm	with throughput of 28 Mb/s in ST FDSOI 28-nm technology
4	S. Shivkumar	IEEE, 2011	RC4 stream cipher is used to generate S-box for AES.	increase the complexity and make the differential and linear cryptanalysis
5	I. Hammad	IEEE, 2010	multistage sub pipelined architecture	Achieve higher efficiency in terms of (throughput/area)
6	Yulin Zhang	IEEE, 2010	AES-128 encryption processor	achieve a throughput of 34.7 Gbps at 271.15 Mhz and 2389 CLB Slices with 200 BRAM.

III. ADVANCE ENCRYPTION STANDARD

The features of AES are as follows −

– Symmetric key symmetric block cipher
– 128-bit data, 128/192/256-bit keys
– Stronger and faster than Triple-DES
– Provide full specification and design details
– Software implementable in Xilinx and MATLAB

AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix −

Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration −

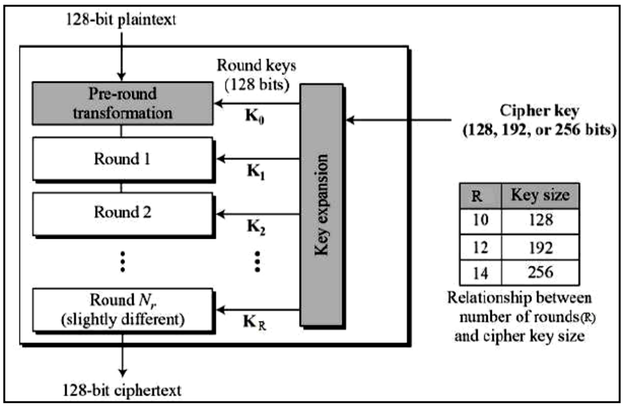

Fig. 2: AES structure

A. Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below −

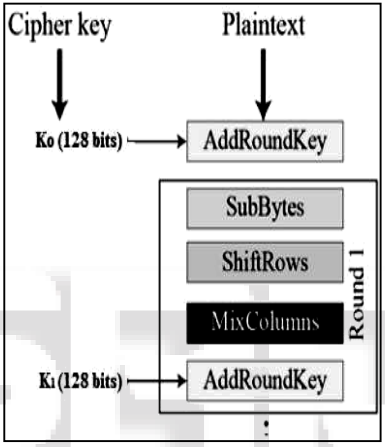

Fig. 3: Byte Substitution

1) Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

2) Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that ‘fall off’ are re-inserted on the right side of row. Shift is carried out as follows −

– First row is not shifted.
– Second row is shifted one (byte) position to the left.
– Third row is shifted two positions to the left.
– Fourth row is shifted three positions to the left.
– The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

3) MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

4) Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

B. Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

– Add round key
– Mix columns
– Shift rows
– Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

1) AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till 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, the AES security is assured only if it is correctly implemented and good key management is employed.

IV. Conclusion

In this paper we surveyed on AES encryption techniques. Performance of AES algorithms vary on different parameters. Generally, with the increase demand of strong security where high level security is needed, we have to compromise with encryption speed in those modifications. Again for encryption of large data like multimedia data, higher encryption speed is needed, for which security is somewhere to be compromised to achieve higher encryption speed. These modifications are useful in different conditions according to the situation demanded. Therefore modifications on AES should focus on designing such methods and techniques that could be used on existing applications in an efficient manner and provide us a highly secured, extremely fast encryption system which can provide high security against all attack including Statistical attack and Brute Force attack and also encrypt large data including multimedia data at very high speed.

References

[1] R. Paul and S. Shukla, "Partitioned security processor architecture on FPGA platform," in IET Computers & Digital Techniques, vol. 12, no. 5, pp. 216-226, 9 2018.

[2] R. Lumbiarres-López, M. López-García and E. Cantó-Navarro, "Hardware Architecture Implemented on FPGA for Protecting Cryptographic Keys against Side-Channel Attacks," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 898-905, 1 Sept.-Oct. 2018.

[3] D. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 25, no. 12, pp. 3281-3290, Dec. 2017.

[4] S. Shivkumar and G. Umamaheswari, "Performance Comparison of Advanced Encryption Standard (AES) and AES Key Dependent S-Box - Simulation Using MATLAB," 2011 International Conference on Process Automation, Control and Computing, Coimbatore, 2011, pp. 1-6.

[5] I. Hammad, K. El-Sankary and E. El-Masry, "High-Speed AES Encryptor With Efficient Merging Techniques," in IEEE Embedded Systems Letters, vol. 2, no. 3, pp. 67-71, Sept. 2010.

[6] Yulin Zhang and Xinggang Wang, "Pipelined implementation of AES encryption based on FPGA," 2010 IEEE International Conference on Information Theory and Information Security, Beijing, 2010, pp. 170-173.

[7] Z. Wang, T. Arslan and A. Erdogan, "Implementation of Hardware Encryption Engine for Wireless Communication on a Reconfigurable Instruction Cell Architecture," 4th IEEE International Symposium on Electronic Design, Test and Applications (delta 2008), Hong Kong, 2008, pp. 148-152.

[8] Y. Wei, F. Yao, E. Pasalic and A. Wang, "New second-order threshold implementation of AES," in IET Information Security, vol. 13, no. 2, pp. 117-124, 3 2019.

[9] M. Xie, S. Li, A. O. Glova, J. Hu and Y. Xie, "Securing Emerging Nonvolatile Main Memory With Fast and Energy-Efficient AES In-Memory Implementation," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 11, pp. 2443-2455, Nov. 2018.

[10] P. A. Naidu and P. K. Joshi, "FPGA implementation of fully pipelined Advanced Encryption Standard," 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, 2015, pp. 0649-0653.

[11] Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1218-1221.

[12] X. Wang, L. Han, C. Wang and X. Liu, "Based MATLAB on Advanced Encryption Standard (AES) IP Validation," 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, 2008, pp. 1329-1331.