INTERNATIONAL JOURNAL OF COMPUTING, SCIENCE AND NEW TECHNOLOGIES (IJCSNT)

VOL. 4 NO. 2 SEPTEMBER 2024

IMPLEMENTATION ANALYSES AND EVALUATION OF SECURITY ALGORITHMS WITH RFID TECHNOLOGY

by

Isizoh A.N[1], Providence Mathias[2], Eze Ukamaka J.[3], Ebih U. J.[4]

1, 2,4: Dept. of Electronics and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria.

3: Dept. of Computer Engineering, Madonna University of Nigeria, Akpugo Campus, Enugu State, Nigeria

ABSTRACT

The rapid advancement of Radio Frequency Identification (RFID) technology has revolutionized the field of automated identification, enabling the efficient and wireless retrieval of data from RFID tags. Despite its widespread adoption, the inherent vulnerabilities associated with RFID systems—such as eavesdropping, snooping, cloning, and unauthorized tracking—necessitate robust security measures to ensure data protection. This paper explores the application of various cryptographic algorithms, including symmetric and asymmetric encryption techniques, within RFID systems to bolster security. In particular, the study emphasizes the implementation of the Advanced Encryption Standard (AES) in RFID technology, addressing the unique challenges of limited processing time, small area, and low power consumption inherent to these systems. By analysing network security algorithms such as DES, AES, RSA, and hash functions like MD5 and SHA-512, this paper aims to evaluate their effectiveness in safeguarding RFID communications. Additionally, it explores integrating digital signatures, email security, and IP security protocols like ESP and AH, contributing to a comprehensive understanding of secure RFID deployments. Through this analysis, the research aspires to propose optimized cryptographic solutions that enhance the security and privacy of RFID systems across various applications.

Keywords/phrases: Network Security, encryption, digital signatures, authentication, cryptographic algorithm

1. INTRODUCTION

Radio Frequency Identification (RFID) is a fast-growing technology in the world today. RFID is an automatic identification method that can remotely retrieve data using devices called RFID tags or transponders. The technology which enables the electronic labelling and wireless identification of objects using radio frequency communications is RFID. The term RFID is used to describe various technologies that use radio waves to automatically identify people or objects. RFID technology is similar to the bar code identification systems we see in retail stores every day. However, one big difference between RFID and bar code technology is that RFID does not rely on the line-of-sight reading that bar code scanning requires to work. It can be done from any angle. RFID tags store unique identification information of objects and communicate the tags so as to allow remote retrieval of their ID. RFID technology depends on the communication between the RFID tags and RFID readers. The main benefits of RFID systems are that they can provide automated contactless identification of a range of physical entities, and can be used to track valuable objects Tassos, D, 2009). RFID and mobile telecommunications are the services that provide information on objects equipped with an RFID tag over a telecommunication network. Tags are stationery and Readers are in mobile phone (mobile). RFID readers can simultaneously scan and also identify hundreds of tagged items (UK Essays, 2018).

From the way in which RFID tags operate via a wireless radio communications channel, there is a concern about privacy and security, including the possibility of eavesdropping, snooping, cloning, counterfeiting and tracking of end users since information stored in tags can easily be retrieved by hidden readers, eventually leading to violation of user privacy and tracking of individuals by the tags they carry (Ahsan et al. 2010). One of the best ways to provide security and privacy measures is through an

authentication process. Authentication is an assurance of the identity of an entity at the other end of communication channel. There are various authentication schemes or protocols such as Password protection which is an example of weak authentication and strong authentication schemes such as those based on a challenge and response concept (Ahsan, et al. 2010). Many RFID authentication protocols use cryptographic techniques to protect messages exchanged over a radio frequency interface from eavesdropping. Compared to asymmetric or public key alternatives, a symmetric key is generally less complicated, requires a smaller number of operations, and can have the same security strength as its asymmetric equivalence using a key of smaller size. These facts make the symmetric key approach more suitable for limited resource RFID systems (Parkash, et. al. 2012).

Network security is a concept of securing data through wireless transmission with the help of cryptography. The Network administrator performs the task of securing data while transmission, avoid unauthorized access of data, avert data misuse and modification of network resources. Network security is used in various computer network sectors such as private and public. Networks used in the organizations, enterprises, institutions etc. are in the form of private or public. Network security is required for all hardware and software function. Administrative and management is necessary to provide protection for hardware and software. Cryptography is concept of securing data with the help of secret keys. Cryptography is the encryption and decryption of data with secret keys using various algorithms. Network security is material part of information security. It is important to secure information passing through network, computers (Umar, et al. 2014).

II. LITERATURE REVIEW

2.1 How RFID System Works

Most RFID systems consist of tags that are attached to the objects to be identified. Each tag has its own "read only" or "rewrite" internal memory depending on the type and application. Typical configuration of this memory is to store product information, such as an object's unique ID manufactured date, etc. The RFID reader generates magnetic fields that enable the RFID system to locate objects (via the tags) that are within its range. The high-frequency electromagnetic energy and query signal generated by the reader triggers the tags to reply to the query; the query frequency could be up to 50 times per second. As a result, communication between the main components of the system i.e., tags and reader are established. As a result, large quantities of data are generated. Several protocols manage the communication process between the reader and tag. These protocols (ISO 15693 and ISO 18000-3 for HF or the ISO 18000-6, and EPC for UHF) begin the identification process when the reader is switched on. These protocol works on selected frequency bands (e.g., 860 – 915 MHz for UHF or 13.56 MHz for HF). If the reader is on and the tag arrives in the reader fields, then it automatically wakes-up and decodes the signal and replies to the reader by modulating the reader's field. All the tags in the reader range may reply at the same time, in this case the reader must detect signal collision (indication of multiple tags). Signal collision is resolved by applying anti-collision algorithm which enables the reader to sort tags and select/handle each tag based on the frequency range (between 50 tags to 200 tags) and the protocol used. In this connection the reader can perform certain operations on the tags such as reading the tag's identifier number and writing data into a tag. The reader performs these operations one by one on each tag. A typical RFID system work cycle can be seen in figure 1(Ahsan, et.al. 2010).

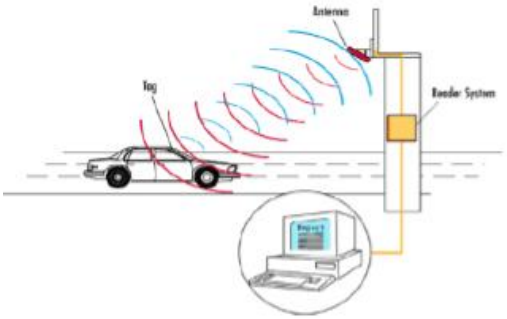

Fig. 1: A typical RFID System

2.2 RFID Components

A combination of RFID technology and computing technology is called RFID system as shown in figure 2. A RFID system consists of following components:
1. Tag/Transponder (electronic label).
2. Antenna (medium for tag reading).
3. Reader /Interrogator (read tag information).

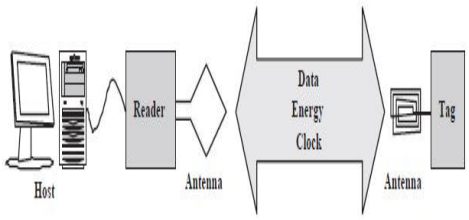

Figure 2: Basic RFID systems

Transponder (Tags)

An RFID tag is a small electronic device that is also referred to as a transponder. The tag consists of a simple silicon microchip and antenna. The tag can be attached to an object, typically an item, box. Information is collected by chip and can be transmitted wirelessly. RFID tag can be active (with batteries), passive (without batteries) and semi-passive (hybrid). Tag has an identification code that can be transmitted towards reader (Parkash, et. Al, (2012).

Classification of RFID tags in relation to power or energy

1. Passive: Also called "pure passive". It obtains operating power from a reader (Parkash, et. Al, (2012). This means that the reader has to keep up its field until the transaction is completed. Because of the lack of a battery, these tags are the smallest and cheapest tags available; however, it also restricts its reading range to a range between 2mm and a few meters. As an added benefit those tags are also suitable to be produced by printing (Christoph, 2013). The reader sends electromagnetic waves that induce a current in the tag's antenna, the tag reflects the RF signal transmitted and adds information by modulating the reflected signal (Parkash, et. Al, (2012). Furthermore, their lifespan is unlimited since they do not depend on an internal power source (Parkash, et. Al, (2012).
2. Semi-passive: These tags have an internal power source that keeps the microchip powered at all times. There are many advantages: Because the chip is always powered it can respond faster to requests, therefore increasing the number of tags that can be queried per second which is important to some applications. Furthermore, since the antenna is not required for collecting power it can be optimized for backscattering and therefore increasing the reading range. And last but not least, since the tag does not use any energy from the field the back-scattered signal is stronger, increasing the range even further. Because of the last two reasons, a semi-active tag has usually a range larger than a passive tag.
3. Active: Like semi-active tags they contain an internal power source but they use the energy supplied for both, to power the microchip and to generate a signal on the antenna. Active tags that send signals without being queried are called beacons. An active tag's range can be tens of meters, making it ideal for locating objects or serving as landmark points. The lifetime is up to 5 years (Parkash, et. Al, (2012). Generally, ensures a longer read range than passive tags. More expensive than passive tags (Parkash, et. Al, (2012).

Classification of RFID tags by the tag's memory type

1. Read-only: The memory is factory programmed, and cannot be modified after it has been manufactured. Its data is static and a limited amount of data can be stored. It is cheaper than read-write tags (Parkash, et. Al, (2012).
2. Read-write: Can be as well read as written into and data can be dynamically altered (Parkash, et. Al, (2012).

Classification of RFID tags by the method of wireless signal used for communication between tag and reader

1. Induction: Close proximity electromagnetic or inductive coupling-near field. Uses LF and HF frequency bands (Parkash, et. Al, (2012).
2. Propagation: Propagating electromagnetic waves-far field. Operate on the UHF and microwave frequency bands (Parkash, et. Al, (2012).

RFID Antenna

RFID antennas are used to collect information about any item. There are many types of RFID antenna like patch antennas, linear polarized antennas, stick antennas and adaptive antennas, gate antenna, and Omni directional antennas. RFID antenna is shown in Figure 3.

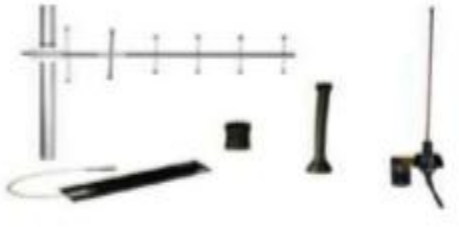

Figure 3: RFID antenna

According to the researchers, an RFID antenna should satisfy the following requirements:

(i) Its size should be small
(ii) It should have omnidirectional or hemispherical coverage
(iii) It must provide maximum possible signal to the microchip
(iv) It should be robust
(v) It should be very cheap.

RFID Reader

Third component of RFID system is RFID reader. The reader sometimes called an interrogator or scanner sends and receives RF data to and from the tag via antennas. A reader may have multiple antennas that are responsible for sending and receiving radio waves. Reader informs data processing system about presence of tagged item. It consists of three main parts: control section, high frequency interface and antenna. Read range of reader is affected by number of factors. Antenna gain, frequency used, orientation of antenna will affect read range. Reader comes in four types: Read, Read/write, fixed and mobile. First two are based on design and technology used and last two are based on fixation of device.

Classification of RFID reader by design and technology used:

1. Read: It is usually a micro-controller-based unit with a wound output coil, peak detector hardware, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation. Only reads data from tag. Different types for different protocols, frequencies and standards exists.
2. Read/write: Reads and write data from/on the tag.

Classification of RFID reader by fixation of the device

1. Stationary: The device is attached in a fixed way, for example at the entrance gate, respectively at the exit gate of products.
2. Mobile: In this case the reader is handy, movable device (Parkash, et. Al, (2012).

Operating Frequencies

Different types of RFID systems operate at different radio frequency. Each radio frequency has its own read distance, power requirements and performance. The choice of frequency depends on the application. Mostly four types of frequencies are used in RFID technology:

A. Low frequency (125-134 KHz)
B. High frequency (13.56 MHz)
C. The ultra-high frequency (902-928 MHz)
D. Microwave (2.4 GHz-2.5 GHz)

2.3 Network Security Algorithms

2.3.1 Symmetric key algorithm

A. DES (Data Encryption Standard)

For the encryption of electronic data, Data Encryption Standard (DES) is used. It is a symmetric key algorithm. Although it is very not secure because of its key length which is short of 56 bits which is criticized by the applications. Methods to crack block ciphers DES were considered to have been a catalyst for the study of cryptography. It can be said that it has jump-started the non-military development and study of

encryption algorithms. Except for the cryptographers in military and intelligence, there were very few cryptographers in the 1970s also very little study of cryptography. Nowadays there are many cryptologists and mathematics departments which have strong programs in cryptography. A whole generation of cryptanalysts has tried to crack the DES algorithm (Ms. Vinaya, 2020).

B. AES (Advanced Encryption Standard)

AES is an algorithm for electronic data which was established by the U. S. National Institute of Standard and Technology AES Advanced Encryption Standard in 2001. The algorithm is asymmetric key algorithm, means that not different but same key is used for encrypting as well as decrypting the data. Taken from a design principle called as a substitution permutation network AES is generated. It is useful in hardware and software. As DES used Feistel network, AES does not. AES algorithm has 128 bits block size, key of 128,192 or 256 bits which is fixed (Ms. Vinaya, 2020)

.

2.3.2 Asymmetric key algorithm

a) RSA(Rivest-Shamir-Adleman)

Rivest-Shamir-Adleman is one of the first public cryptography systems. It's used for secure data transmission. The encrypting key in this system is not kept private. It is based on the difficulty of product factorization of two prime numbers which are large in size. This algorithm has 4 steps. They are key generation, key distribution, encryption, and decryption (Ms. Vinaya, 2020).

2.3.3 Hash Function Algorithm

1. MD5

This MD5 Message digest algorithm produces 128-bit Hash values. This was suffering from extensive vulnerabilities. In the beginning, it was used as a cryptographic hash function. MD5 is new one, used to replace the MD4 hash function. Later on, it is specified as RFCI-321. From 2019 it is used widely. MD5 is used in software. It gives assurance to intact transferred file. By this user compares checksum of the downloaded file. In distribution packages MD5 sum is used. "Get-File-Flash" installs Microsoft utilities. MD5 provides error checking. Corrupt and incomplete download is checked by using MD5. In electronic discovery, it is used. Variable length message is fixed in length output of 128 bits in MD5.Then blocks of 512 bits are prepared of input message. Message is padded first a single bit one is appended to the end of message. MD5 algorithm is divided into four 32 bits word. Main algorithm uses each 512 bits message block to modify the state (Ms. Vinaya, 2020).

2. SHA-512

SHA – 512 performs on data given to it. It plays important role in digital security and cryptography. It is simple math with diagrams. SHA -2 including SHA -256, it is group of hashing algorithms. Input data is produced as output of fixed length. Hash function should be that which divides output value equally.SHA512 has an input size limit. Original message, padding bits, padding size are three parts of message. Default value is used to start off the process for the first block it is stored somewhere for next use final hash digest has used for processing phase of SHA-512 for the intermediate result. It is done upon formatted input. 1024-bit block and result of previous processing is taken in this method. Message block is expanded in words by utilizing message sequencer. Intermediate results are taken for processing the next block. SHA-512 algorithm is used for processing the original message. It is one part of hashing algorithm (Ms. Vinaya, 2020)..

3. HMAC

HMAC is a special type of message authentication code. Secret key is used to derive two key inner and outer. This provides better immunity against length extension attacks. The cryptographic strength of HMAC is as per the size of the secret key. Brute force is sometimes used to uncover the secret key this is a defect in this method. Since 2011 abstract theory and

source code have been used (Ms. Vinaya, 2020).

2.3.4 Digital Signature Algorithm

This algorithm has two keys, public and private. To generate the digital signature, private key is used which can be checked by the given public key. This signature helps authenticate messages, integrity and non-repudiation. This algorithm has mainly four operations: key generation, distribution, signing and verification of signature.

2.3.5 Web Security Algorithm

SSL algorithm

Secure Socket Layer Algorithm (SSL) is an encryption algorithm which is designed to communicate between the network layer and application layer of networks. It provides security to communicate interaction models such as client side and server side. The SSL algorithm provides security services such as confidentiality, digital signature, web security. SSL uses cryptographic system to secure data with the usage of private and public keys. The working of the SSL algorithm is done with the help of SSL handshake. It uses both symmetric and asymmetric cryptography. Before the sending data from browser to server firstly the verification is done using SSL certificate. Firstly, client sends required information to the server. The server also responds to the information received from the client. The client verifies the SSL certificate which is authenticated from Certificate Authority. If the authentication flops, then client declines the connection. If the authentication succeeds, then it proceeds. The client induces a secret key and encrypts the data with the server's public key and dispatches to server. If server wants to verify the authentication of client server request it to client and client sends certificates to server. The decryption of session key through server is done by its private key and then dispatched to the client with the encrypted of session key. It is serviced in credit cards, login, and for browsing social media (Ms. Vinaya, 2020).

SET Algorithm

Secure Electronic Transaction is a type of electronic transactions which itself explains that it is used for the online financial transaction communication. SET algorithm is used for the purpose of security protocols and formats as SSL, STT and S-HTTP. It is not a type of online payment system. The key features of SET are that it provides

i) confidentiality to information requested and stored
ii) integrity of data provided
iii) cardholders bank account approval
iv) Service provider merchant authentication.

The SET algorithm protocol works as follows: When customer opens an account with a bank it obtains bank card known as debit card, credit card named as master card, rupay, visa etc. for the purpose of online transactions. After the verification of customer's identity, it receives digital certificate which is verified by the asymmetric public key of RSA and the expiration date of thebank cards. Merchants too have their certificates. Merchant has possession of two certificates for two public keys one for signing messages and one for key exchange. The customer order process involves the browsing of merchant's website to buy the products. Customer sends the list of purchasing items to merchant who returns a product lists form. Along with product list merchant sends the duplicate copy of certificate to customer so that they canverify authorized valid store. Customer sends order lists and billing details of credit cards along with customer's certificate. The details of payment are sent to merchant in encrypted way so that merchant also can't read and the customer is also verified by merchant. Finally, merchant sends request to customer for payment confirmation so that customer is able to do sufficient purchase. After the confirmation of payment authorization order confirmation is send to customer and the purchased products or services are delivered to the customer (Ms. Vinaya, 2020).

2.3.6 Email Security Algorithm

1) PGP

Pretty Good Privacy (PGP) is hybrid cryptosystem extremely used for security of emails which provides the services of

i) confidentiality through encryption
ii) authentication with use of digital signature
iii) compression

iv) compatibility
v) segmentation of mails

PGP works on four types of keys for the encryption and decryption of emails. The main function provided by this algorithm is to send safe and secured data through mails.The PGP encryption works on the important concept of symmetric-key, public-key cryptography and digital signatures. Firstly the encrypted plain text is compressed using PGP. PGP uses secret key which is used only one time. The random numbers are generated using this key which is used for encrypting plain text into cipher text. After the mails are received by receiver then session key is used as public key to encrypt the data on receiver's side. Decryption is done in the reverse manner of encryption (Ms. Vinaya, 2020).

2.3.7 IP Security Algorithm

a. ESP

Encapsulating security payload (ESP) protocol is used in internet protocol security. The services provided by the protocols are confidentiality through encryption, authentication through use of public key, antireplay services through sequence number mechanism and limited traffic low confidentiality through security gateways. ESP uses both tunnel and transport mode to process the encrypted data. The components of ESP header are

i) security parameter index(SPI)
ii) sequence number
iii) payload data
iv) authentication data
v) next header
vi) padding
vii) Padding length.

ESP does not protect the data header to protect it in tunnel mode the overall packet is enclosed in different new packet so the header data can be also get protected by any misuse.

b. AH

Authentication header protocol is used in internet security protocol. AH provides the security services as integrity for IP datagram, authentication for IP datagram, no repudiation and replay attacks. The components of AH protocol are

i) next header
ii) payload length
iii) authentication data
iv) reserved
v) security parameter index
vi) Sequence number.

In tunnel mode the IP packet which contains header data is also encrypted. AH can be used in the combination of ESP or in a nested fashion. AH provides anti-replay mechanism at discretion of receiver to protect data from service attacks (Ms. Vinaya, 2020).

III. RESEARCH ANALYSES

3.1 AES (Advance Encryption Standard) Implementation in RFID

The need for strong encryption in RF tags has increased in recent years. The most popular encryption algorithm is the Advance Encryption Standard (AES), which is certified by the U.S. National Institute of Standards and Technology (NIST). RFID tags with AES encryption are being adopted as a secured encryption standard in the industry. The two frequency ranges in which AES encryption is widely used are low frequency range (LF, 120-150 kHz) and high frequency range (HF, 13.56 MHz). These two applications have different constraints in terms of encryption time. The LF applications require encryption to finish within a few hundred RF cycles, In HF applications, AES processing time can be as long as several thousand RF cycles. This paper describes the implementation of 128-bit AES encryption in custom design RFID chips under the processing time constraint for the two frequency ranges. Another two important constraints of ASIC design are also taken into account: small area and low power consumption. For LF applications where the processing time is limited, a hardware module is proposed. For HF applications, a custom microcontroller unit with an encryption program is proposed in order to provide programmability. The software version for encryption also saves

chip area since it does not require extra hardware.

AES is a block cipher that converts plain text input with length of 128, 192, or 256 bits into cipher text output with the same length. The input text is processed as a two-dimensional array of bytes illustrated in Fig 4, which is extracted from [10]. The intermediate data are called States. The States are processed by four transformations: Sub Byte, Shift Rows, Mix Column, and Add Round Key. The AES encryption and decryption flow chart, as presented in (Mangard, 2003), is shown in Figure 5.

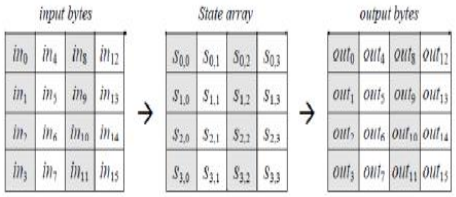

Figure 4: AES Encryption Data Format

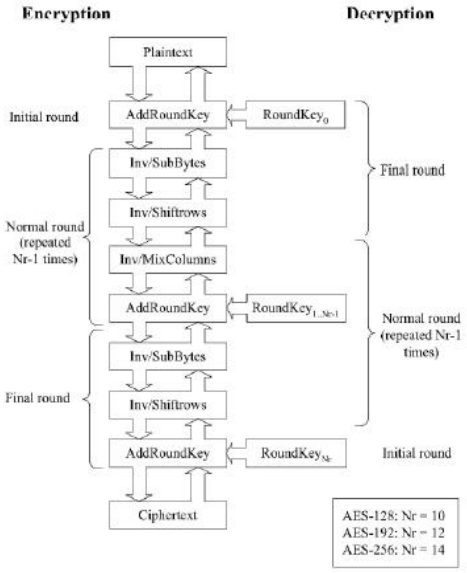

Figure 5: AES Encryption and Decryption Flow Chart

3.2 AES Hardware Implementation

The advantage of the hardware module over its software counterpart is that it can process encryption and decryption faster. The disadvantage is that the module occupies extra chip area. The data path of this hardware module relies on the architecture presented in (Mangard, 2003). This architecture is intuitive and modular, which allows easy customization and optimization.

A. Top Module Block Diagram

The top module architecture is shown in Fig 6. The AES_Top unit consists of three main units: Data Unit, Key Gen and Control.

B. Data Units

The structure of the Data Unit is shown in Figure 7. The Data Unit consists of sixteen Data Cells, four SBox, modules, and one MCol module.

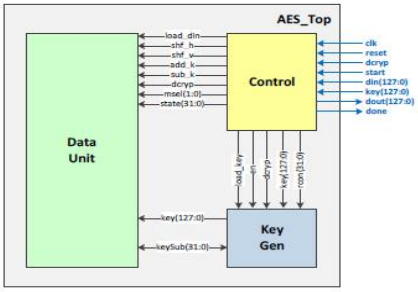

Figure 6: Block Diagram of the AES Hardware Top Module

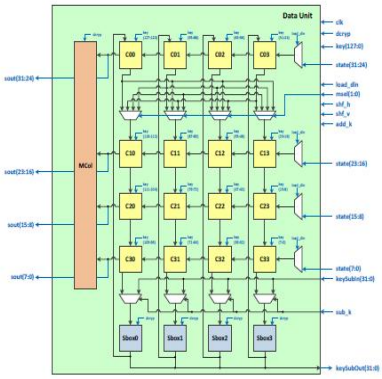

Figure 7: Block Diagram of the Data Unit

Data Cell

The Data Cell contains one byte of the. The Data Unit contains 16 Data Cells arranged as a 4x4 array. A Data Cell has three functions: load horizontal input, load vertical input, and add key to the State.

SBox

SBox converts the input byte using multiplicative inversion and affine transformation. The input bytes are shifted down

to the four SBoxes four bytes at a time during SubByte process. Therefore, the SubByte process takes four clock cycles to complete.

SBox can be implemented by storing pre-calculated data in a look-up table. However, the look-up version of the SBox is very big; the four SBoxes take about 46% of the AES module area. In order to reduce the size of the SBox, we implement it according to its mathematical definition: multiplicative inversion and affine transformation in GF(28).

The details of SBox implementation can be found in. The overview of the module is shown in Fig 6. In case of encryption (INV = 0), the input goes into the multiplicative inversion module before going into affine transformation (AT) module. In case of decryption (INV = 1), the input goes into the inverse affine transformation (AT-1) module before taking the multiplicative inverse.

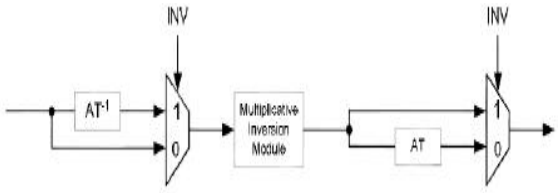

Figure 8: Block Diagram of the SBox Module

C. Key Generator

Before starting AddRoundKey transformation, the controller must load the AES key into the generator. Then enable it to produce RoundKey. Key generation takes one clock cycle for each round.

In case of decryption, the Controller must load the AES key, enable the Key Generator to run forward until the last RoundKey is generated, after which it calculates the next RoundKey in reverse order. This forward calculation process takes 10 additional clock cycles.

The structures of the Key Generator in case of encryption and decryption are shown separately in Figure 9 and 10, although they are actually implemented with a single hardware module.

D. Controller

The Controller is a 6-state Finite State Machine. The operation of each state is explained in Table I. The state diagram during encryption and decryption are provided in Figure 11 and Figure 12. Each normal AES round takes nine clock cycles to complete, while the first round and the last round takes one and six clock cycles respectively. The total encryption time is 93 clock cycles, while the decryption time is 103 clock cycles.

Table 1. Operating States of the Controller

State	Description	Processing Time (clk)
IDLE	Wait for Start signal	-
LOAD	Load input data into Data Unit, and load AES key into Key Generator. During decryption, it needs 10 extra clock to generate the last RoundKey	Encrypt: 4 Decrypt: 14
ADD_RKEY	Perform AddRoundKey operation	1
SUBBYTE_ SHFROW	Perform SubByte and ShiftRow by shifting the State down.	4
MIXCOL	Perform MixColumn operation by shifting the State to the left.	4
DONE	Generate done signal to indicate end of operation	-

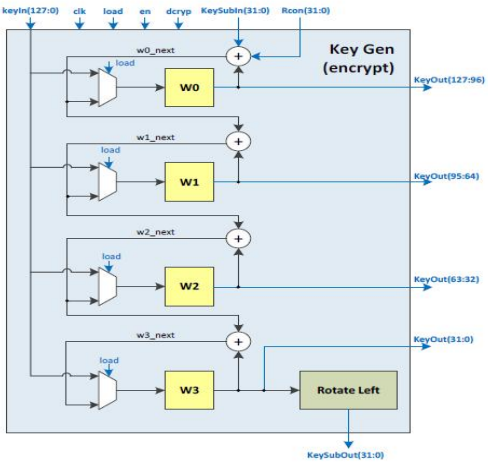

Figure 9: Block Diagram of the Key Generator during Encryption

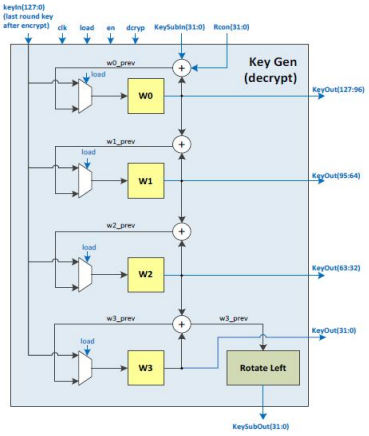

Figure 10: Block Diagram of the Key Generator during Decryption

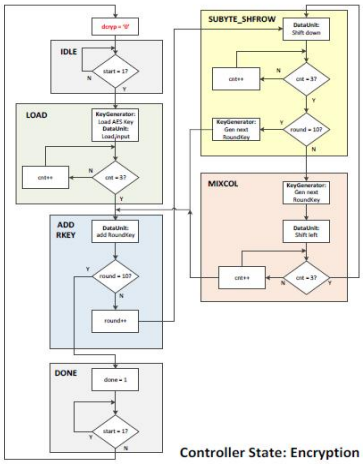

Figure 11: State Diagram of the Controller during Encryption

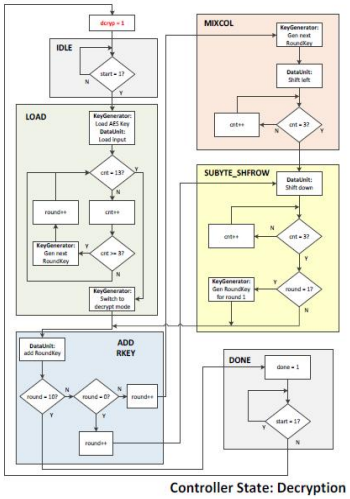

Figure 12: State Diagram of the Controller during Decryption

E. AES Hardware Characteristic

The module AES_top is synthesized with the digital synthesis tool with 0.13um CMOS technology. The power consumption is measured by exporting the synthesized design to a netlist and simulating it using a netlist simulator. The supply voltage is 1.5V and the clock frequency is 125 kHz.

IV. CONCLUSION

Due to the fact that RFID systems are becoming so popular in data networking, it is therefore necessary to consider the security issues that come out from the implementation or design of new applications and systems. These problems are related to data privacy, integrity, and secrecy. The security algorithms reported in this paper are designed with user authentication and encryption algorithms. The chosen authentication scheme is the mutual authentication protocol. By this way, the first attack in RFID systems, unauthorized reading of the information stored in tags, can be neutralized. In this new approach, the initialization vector is not transmitted; therefore, it is generated in each entity. That is, the generation of the IV is done by a lineal increment of its value for each data frame transmitted, and accordingly, we obtain different values for the dynamic key KK. By this way, the second attack in RFID systems, eavesdropping transmissions, can be neutralized.

Note that the low cost demanded for RFID tags causes them to be very resource-limited and therefore encryption algorithms like DES or AES that require more than 20000 gates are not practical. Furthermore, power restrictions should be taken into account since most RFID tags in use are passive (Tassos, 2009). Finally, an extension of the work presented in this paper could be the implementation of an RFID network considering anti-collision protocols.

REFERENCES

Ahsan, K., Shah, H., & Kingston, P. (2015). RFID applications: An introductory and exploratory study. *IJCSI International Journal of Computer Science Issues*, 7(1), 3.

Parkash, D., Kundu, T., & Kaur, P. (2012). The RFID technology and its applications: A review. *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJECIERD)*, 2(3), 109-120.

Farooq, U., Hasan, M., Amar, M., Hanif, A., & Asad, M. U. (2014). RFID-based security and access control system. *IACSIT International Journal of Engineering and Technology*, 6(4).

Jechlitschek, C. (2013, November). *A survey paper on radio frequency identification trends*.

Tassos, D. (2009). *RFID security and privacy*. In R. Leszczyna (Ed.), RFID security: Techniques, protocols and system-on-chip design (pp. 1-23). Springer. https://doi.org/10.1007/978-0-387-76481-8_1

Israsena, P. (2005). Design and implementation of low power hardware encryption for low-cost secure RFID using TEA. In *Fifth International Conference in Information, Communications and Signal Processing* (pp. 1-5). Bangkok, Thailand.

Kulkarni, V., Kirdat, S., Patil, S., & Patil, C. H. (2020). Study on network security algorithm. *International Journal of Engineering Research & Technology (IJERT)*, 8(5).

UKEssays. (November 2018). History And Evolution Of RFID Technology Information Technology Essay. Retrieved from https://us.ukessays.com/essays/informationtechnology/history-and-evolution-of-rfid-technology-information-technology-essay.php?vref=1

