VLSI IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHMS IN INTERNET OF THINGS

[1]J.GOPIKA RAJAN, [2]ASWATHY K NAIR

[1,2]Electronics and Communication Department, Amrita School of Engineering, Karunagapally, India

Abstract- Internet of Things (IOT) is an advanced version of Internet where it is not just the mobile phones and computers that is connected to internet but also the other electronic objects also get connected to internet. Internet of Things (IOT) requires the use of IPv6 protocol to satisfy address needs of large number of surrounding things. The challenge faced in this wireless mode of communication between devices is the security of information & the privacy of individuals. In this paper a cryptographic method is put forth which makes use of MD5 and AES algorithm to attain security & privacy. Both these algorithms are simulated in Modelsim 6.5 and Xilinx 14.2 tool using verilog HDL. Proposed method of chaining of the two algorithms twice provide better security and privacy. On integrating these algorithms into an RFID tag a secure means of communication can exist between surrounding things and thus making way for the acceptance of Internet of Things in society.

Index terms: Internet of Things; RFID; AES; MD5; confidentiality; integrity; VLSI.

I. INTRODUCTION:

The vision of IOT is to extend Internet into our day to day life and create a physically networked world in which all electronic devices are connected via a wireless network to form a globally intelligent infrastructure. All the objects within the network are electronically tagged using an RFID tag so as to identify, access, control & manage the functionality of other objects. Thus IOT establishes a huge network of interconnected objects where objects can communicate with humans as well as other objects. These objects, which are fitted with RFID tag ,are prone to several attacks due to the lack of a physical contact in the communication process which cause loss of individual privacy and security of information. A solution to this issue of security and privacy had not yet been developed. Through this paper a method has been put forth to meet this challenges of security and privacy of data and individuals respectively.

The rest of the paper is organized according to the following outline. In section 3 cryptographic algorithms Rinjadael AES algorithm and MD5 Hash algorithm isdiscussed. Section 3 puts forward a method to integrate the cryptographic algorithm into the RFID tag. Section 4 highlights the reason for integrating the cryptographic algorithms to RFID. And in section 4 the experimental results and observations of implementing the cryptographic algorithms in Xilinx 14.2 is shown.

The various enabling technologies of Internet of Things such as (Radio Frequency Identification) RFID, (Wireless Sensor Networks) WSN , (Real-time location systems)RTLS is discussed in paper [1] .The various challenges of IOT that must be overcome to get the required social acceptance is also mentioned. Paper [2] puts forward an approach based on the Internet of Things technology in medical environment to attain a secure connectivity with patient sensors and everything around patient.

A supply chain information transmission model based on RFID and Internet of Things is proposed in paper [3].

Authors of [4, 5] describes on the simulation of AES algorithm as well as its implementation in hardware.

In paper [6] a general architecture and several implementations of MD5 hash algorithm are presented.

Paper [7] highlights the various security requirements of RFID along with an application specific security measures. Also the challenges and perspectives for future improvements of security measures in RFID systems and privacy issues are outlined.

Authors in [8] emphasizes that security and privacy are the key issues of IOT applications and provides a research analysis of key technologies including encryption mechanisms, communication security, cryptographic algorithm, etc and outlines it challenges.

II. SYSTEM MODEL FOR RFID TECHNOLOGY

Radio Frequency Identification (RFID) is a wireless technology which is used to identify a unique object/persons and to track the data regarding that object/person. It is the information collection terminal and information entrance terminal of IOT after reading and processing the data stored in the RFID tags. The RFID tag and RFID reader establishes a radio frequency channel through which data transfer takes place. Considering the advantages of RFID technology such as contactless, speediness, multiple object identification, etc along with its applications in industries, medical, transportation, etc the integration of RFID in IOT provides an added support to improve the quality of living. The RFID reader continuously emits RF waves. When a RFID tag encounters the RF wave the tag transfers its unique ID code to the reader which then sends the code server. After which the information about that object in which the tag was present is transferred.

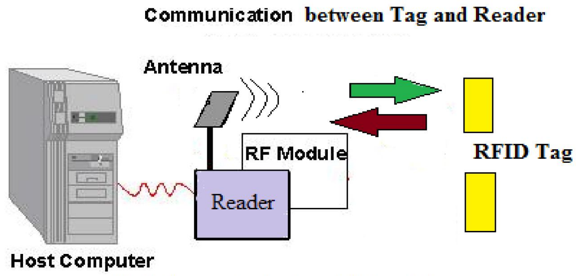


Fig 1: Communication in an RFID module.

With the deployment of advanced technologies the security issues concerned with the latest technology must also be addressed along with the issues related to the interaction of the technology with the existing products. The security of the system is to be optimized to avoid the mishandling of RFID technology. Authenticity, confidentiality, integrity, data privacy are some of the security requirements that need to be considered in an RFID system. Therefore cryptographic algorithms need to be integrated into RFID tag to tackle the susceptibility of the existing security issues.

Thus by integrating the above mentioned chained cryptographic algorithms into the tag a secure means of data transfer can take place in IOT.

III. IV.AUTHENTICATION AND INTEGRITY OF RESPONDER DATA IN RFID

The ubiquity of RFID makes it an important component in IOT and this technology connect the physical world with internet world. Many application specific security mechanisms for authentication and confidentiality have been adopted. But the existing security mechanism has to be enhanced for IoT. The data in RFID is prone to different attacks such as spoofing, eavesdropping and denial of service. Since RFID technology doesn't need line of sight unauthorized RFID readers can obtain the data if it is not encrypted. Therefore encryption is done using a chaining method which makes use of AES algorithm and MD5 algorithm. This encrypted data is send to the reader and then to the host computer. Authenticity is guaranteed by the use of MD5 algorithm. The chaining method introduced in this paper is an enhancement of the existing security solution that enables to improve the user authentication, integrity, security and privacy of the information being transferred from tag to reader.

IV. PROPOSED SYSTEM- CHAINING METHOD

Despite all the disadvantages of AES algorithm and MD5 algorithm the combination of both can bring about a significant improvement in the security and privacy issue of RFID technology through which the issue of acceptance of IOT can be solved.

By chaining each of the 512 bits of data is compressed to 128 bits of data and is then encrypted using AES algorithm. This encrypted data is then padded and then appending with the length of bits, that is 128, so that its length reaches to 512 bits. This block of 512 bits is again compressed to 128 bits of data and then encrypted. This process continues for 2 chains of operation. This chaining operation provides better security and privacy.

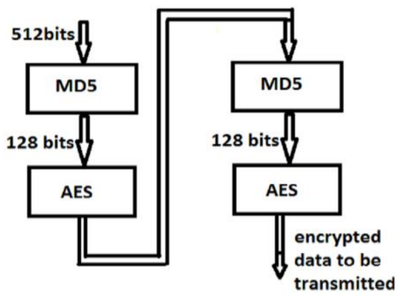


Fig .6. Chaining operation

V. SYSTEM REQUIREMENTS CRYPTOGRAPHIC ALGORITHMS

A . AES

Advanced Encryption Standard(AES) is public key algorithm. It ensures confidentiality and privacy of data. It is based on Rinjadael and takes blocks of data as input i.e 128 bits. For an AES algorithm operating with 128 bits there are about 10 rounds of operation. Broadly, AES has three main operations: key expansion, encryption and decryption. In key expansion the 128 bit data is grouped as four words as shown in fig 2 and each word is substituted with a word from sbox, then the row of words is rotated and then is xored with a constant Rcon whose value depends on the round of operation takes place as shown in fig 3. The various values of Rconst for each round of operation is shown in table 1. The result of key expansion are a set of 10 round keys. In encryption the main process are substitution of bytes using sbox, rotation of the rows, mix column transformation using finite field arithmetic and then xoring with each round key obtained from key expansion routine based on the round of operation. And in decryption the main process are inverse substitution of bytes using sbox, inverse rotation of the rows, inverse mix column transformation using finite field arithmetic and then xoring with each round key obtained from key expansion routine based on the round of operation. This process continues till it completes 10 rounds[5].

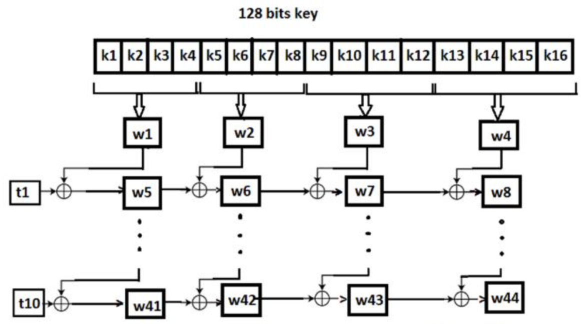


Fig. 2. Key Exapansion (Ref: Cryptography and Network Security, Behrous Ferouzon)

TABLE I : Various Values Of Rconst (Ref: Cryptography and Network Security, Behrous Ferouzon)

Round of operation	Rconst
1st round	$(01\ 00\ 00\ 00)_{16}$
2nd round	$(02\ 00\ 00\ 00)_{16}$
3rd round	$(04\ 00\ 00\ 00)_{16}$
4th round	$(08\ 00\ 00\ 00)_{16}$
5th round	$(10\ 00\ 00\ 00)_{16}$
6th round	$(20\ 00\ 00\ 00)_{16}$
7th round	$(80\ 00\ 00\ 00)_{16}$
8th round	$(1B\ 00\ 00\ 00)_{16}$
9th round	$(36\ 00\ 00\ 00)_{16}$
10th round	

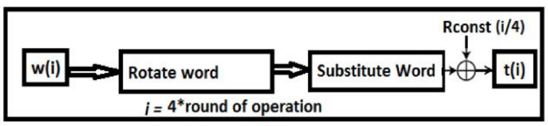


Fig. 3. Step to determine various values of t (Ref: Cryptography and Network Security, Behrous Ferouzon)

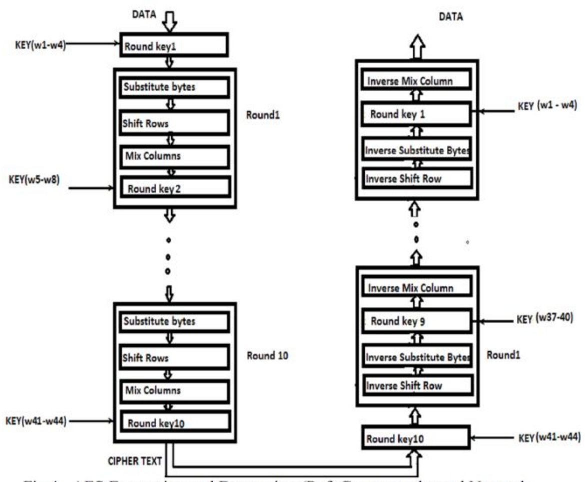


Fig 4 . AES Encryption and Decryption (Ref: Cryptography and Network Security, Behrous Ferouzon)

B. MD5

MD5 is message digest hash algorithm which works with 512 bits of data which is interpreted to a message digest of 128 bits. MD5 algorithm ensures integrity of data. It accepts n bits of data as input and divides it into blocks of 512 bits each but if any of the block of data is less than 512 bits then data is padded with 1 bit followed by 0's, so that resulting number of bits is congruent to mod 448, and is then followed by appending length ,where the length implies the initial length of bits before padding, now the resulting number of bits is congruent to mod 512 .The next step is initializing a MD buffer which is then processed [6] by using various functions as shown in fig 5. MD5 basically consists of 4 rounds of operation with each round having 16 steps of operation. For each round of operation a separate function is used.

The process are as follows:

F(A,B,C,D) = (A && B) || (~ A && B)

G(A,B,C,D) = (A && B) || (B && ~ C)

H(A,B,C,D) = A ⊕ **B** ⊕ C

I(A,B,C,D) = B ⊕ (A || ~ C)

Then the processed message is then compressed to generate a compression function as is shown in fig 6. The various values of T[I] for each step in each round of operation is shown in table 2.

A = D

B = B+(F(B,C,D) + X[K]+T[I]<<S)

C = B

D = C

of all hashing algorithms MD5 is the fastest.MD5 also checks for the authenticity of data.

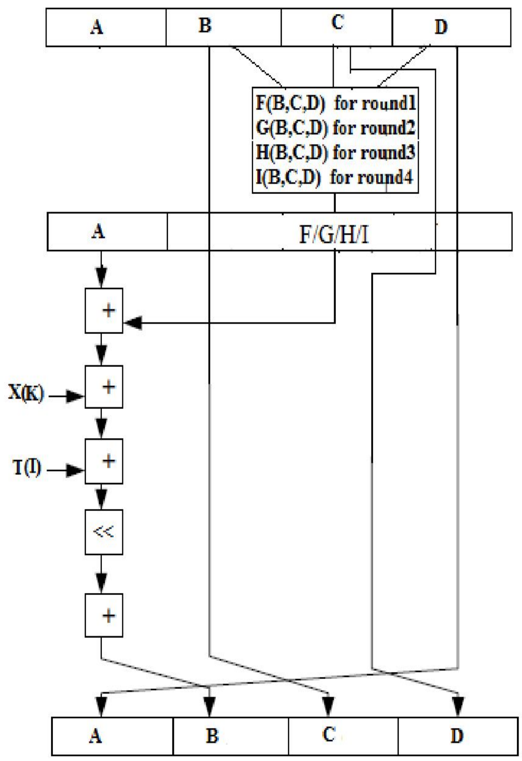


Fig 5: Single step in MD5 [Ref: Paper[6]]

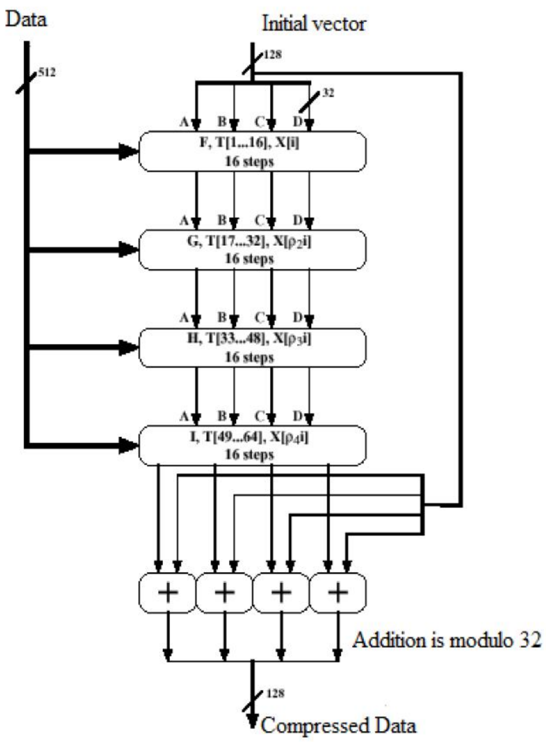


Fig.6. Four rounds of operation[Ref: paper[6]]

TABLE 2: Various Values of T[I]

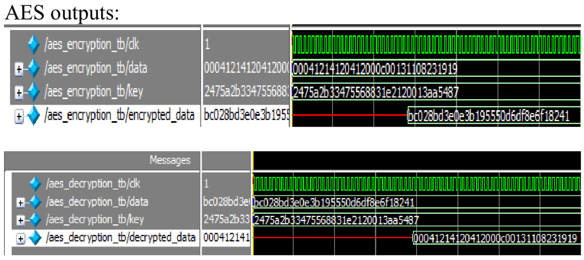
	Value of T[I] for Round1	Round2	Round3	Round4
Step1	d76aa478	f61e2562	fffa3942	f4292244
Step2	e8c7b756	c040b340	8771f681	432aff97
Step3	242070db	265e5a51	6d9d6122	ab9423a7
Step4	c1bdceee	e9b6c7aa	fde5380c	fc93a039
Step5	f57c0faf	d62f105d	a4beea44	655b59c3
Step6	4787c62a	02441453	4bdecfa9	8f0ccc92
Step7	a8304613	d8a1e681	f6bb4b60	ffeff47d
Step8	fd469501	e7d3fbc8	bebfbc70	85845dd1
Step9	698098d8	21e1cde6	289b7ec6	6fa87e4f
Step10	8b44f7af	c33707d6	eaa127fa	fe2ce6e0
Step11	ffff5bb1	f4d50d87	d4ef3085	a3014314
Step12	895cd7be	455a14ed	04881d05	4e0811a1
Step13	6b901122	a9e3e905	d9d4d039	f7537e82
Step14	fd987193	fcefa3f8	e6db99e5	bd3af235
Step15	a679438e	676f02d9	1fa27cf8	2ad7d2bb
Step16	49b40821	8d2a4c8a	c4ac5665	eb86d391

VI. EXPERIMENTAL RESULTS

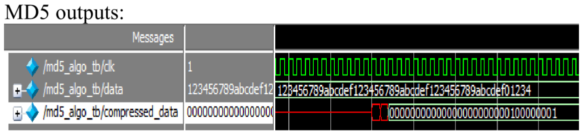
The combination of AES and MD5 encryption and decryption are simulated using VHDL and optimized results are obtained. By make use of the characteristics of AES and MD5 the efficiency of encryption in RFID can be improved.

The delay in the execution of AES is only 4 ns whereas in MD5 the delay is 5.587ns . The output waveforms of AES and MD5 algorithm are shown below:

AES outputs:



MD5 outputs:



The synthesis and timing reports obtained by synthesizing AES and MD5 algorithm is shown below:

AES:

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	9127	69120	13%
Number of Slice LUTs	15599	69120	22%
Number of fully used LUT-FF pairs	9032	15694	57%
Number of bonded IOBs	401	640	62%
Number of Block RAM/FIFO	23	148	15%
Number of BUFG/BUFGCTRLs	1	32	3%

Synthesis Report:
Number of ROMs : 400
Number of Registers : 1382
Number of Slice Registers : 9127

Timing Summary:
Delay : 4.191ns.
Minimum period: 4.191ns
(Maximum Frequency:238.609MHz)
Minimum input arrival time before clock: 4.668ns
Maximum output required time after clock: 4.823ns
Offset time : 4.667ns (levels of logic 7)
Offset time : 4.823ns (levels of logic 2)
Total CPU time : 292.72 secs

Total memory usage : 1291620 kilobytes.

MD5:

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	17472	69120	25%
Number of Slice LUTs	56623	69120	81%
Number of fully used LUT-FF pairs	16448	57647	28%
Number of bonded IOBs	768	640	120%
Number of Block RAM/FIFO	16	148	10%
Number of BUFG/BUFGCTRLs	1	32	3%

HDL Synthesis Report:

Number of ROMs : 64
Number of Adders/Subtractors : 503
Number of Registers : 615
Number of Comparators : 729
Number of XORs : 128

Timing Summary:
Delay : 5.587ns
Minimum period: 5.587ns
(Maximum Frequency: 178.982MHz)
Minimum input arrival time before clock: 4.780ns
Maximum output required time after clock: 2.826ns
Offset: 4.780ns (Levels of Logic = 34)
Offset: 2.826ns (Levels of Logic = 1)
Total CPU time: 207.10 secs

Total memory usage is 915044 kilobytes.

CONCLUSION

An efficient method of cryptographic chaining approach has been introduced in this paper. A secure means of data transfer can take place in IOT by integrating the chained cryptographic algorithms into the tag. The code is simulated in verilog and the efficiency is verified.

A synthesizable verilog code has been developed for the MD5 algorithm and the 128 bit AES algorithm and they have been chained for two rounds of operation and is then simulated in Modelsim6.5 and Xilinx14.2 which can be implemented in an FPGA kit. Individually AES and MD5 has several shortcomings but by the combination of the two algorithms the security improves drastically but at the same time the memory usage increases.

REFERENCES

[1] Iker Mayorodomo, Peter Spies, Fritz Meir , Stephan Otto , Sebastian Lempert, Josef Bernard and Alexander Pflaum “Emerging Technologies and Challenges For Internet of Things ”. 2011 IEEE Conference

[2] Antonio J. Jara, Miguel A.Zamora and Antonio F.G. Skarmeta “An architecture based on Internet of Things to support mobility and security in medical environment” University of Murcia IEEE 2010 CCNC.

[3] Bo Yan, Guangwen Huang "Supply Chain Information Transmission based on RFID and Internet of Things": 2009 ISECS International Colloquium on Computing, Communication, Control, and Management pp 166-169.

[4] Chetan Sangwan ,Chetan Bardwaj ,Nisha ,Taruna Sikka :"VLSI Implementation of Advanced Encryption Standard";2012 Second International Conference on Advanced Commuting and Communication Technologies , pp 412-418.

[5] Rozita Borhan, Raja Mohd Fuad Tengku Aziz ;”Sucessful Implementation of AES algorithm in hardware”.2012 IEEE International Conference on Electronics Design ,Systems and Application (ICEDSA) ,pp 27-32.

[6] Kimmo Jarvinen, Matti Tommiska, Jorma Skytta,“Hardware Implementation Analysis of the MD5 Hash Algorithm”, 38th Hawaii Conference on System Science 2005, pp 1-10.

[7] Ted Phillips, Tom Karygiannis ,“Security Standards for the RFID Market”, IEEE Computer Society, November-December 2005, pp 85-89.

[8] Hui Suo, Jiafu Wan, Caifeng Zou,Jianqi Liu :"Security in Internet of Things : A Review " 2012 International Conference on Computer Science and Electronics Engineering pp 648-651.

★★★