International Journal of Research

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org

Security Authentication through a Near-Field Communication in Asymmetric Cryptography

S Tanveer Ahammad
PG Scholar, Sri Krishnadevaraya Engineering College, Gooty, Andhra Pradesh, India

B. Balasubbanna
Assoc Prof, Sri Krishnadevaraya Engineering College, Gooty, Andhra Pradesh, India.

ABSTRACT

This paper presents the design and implementation of a complete near-field communication (NFC) tag system that supports high-security features. The tag design contains all hardware modules required for a practical realization, which are: an analog 13.56-MHz radio-frequency identification (RFID) front-end, a digital part that includes a tiny (programmable) 8-b microcontroller, a framing logic for data transmission, a memory unit, and a crypto unit. All components have been highly optimized to meet the fierce requirements of passively powered RFID devices while providing a high level of flexibility and security. The tag is fully compliant with the NFC Forum Type-4 specification and supports the ISO/IEC 14443A (layer 1–4) communication protocol as well as block transmission according to ISO/IEC 7816. Its security features include support of encryption and decryption using the Advanced Encryption Standard (AES- 128), the generation of digital signatures using the elliptic curve digital signature algorithm according to NIST P-192, and several countermeasures against common implementation attacks, such as side-channel attacks and fault analyses. The chip has been fabricated in a 0.35-μm CMOS process technology, and requires 49 999 GEs of chip area in total (including digital parts and analog front-end).

Finally, we present a practical realization of our design that can be powered passively by a conventional NFC enabled mobile phone for realizing proof-of-origin applications to prevent counterfeiting of goods, or to provide location-aware services using RFID technology.

Index Terms: 8-b microcontroller; advanced encryption standard (AES); elliptic curve cryptography; elliptic curve digital signature algorithm (ECDSA); embedded system; implementation security; near-field communication (NFC); radio-frequency identification (RFID); VLSI design

1. INTRODUCTION

NFC is a Radio Frequency (RF) technology for communication over short distances up to about 10cm.It is mainly a logical advancement of Radio Frequency Identification (RFID).The history of RFID reaches back to the Second World War, where the British Air force tagged their planes with suitcase-sized devices to establish friend-enemy detection. The first commercial release came in the 1960’s: 1 bit RFID for securing goods in shops, which is still widely used. In the 1990’s RFID became more and more common e.g. for admission control systems or toll systems In 2002, NFC was developed by NXP Semiconductors and Sony. In general, NFC is compatible with existing RFID systems, but its architecture is different in principle. While RFID has only a reader - tag structure, an NFC device can be both reader and transmitter. In 2004, for better standardization the NFC-Forum was founded by the two developing companies. The forum now has about 140 members. After this, the most NFC relevant standards were released as European Computer Manufacturers Association (ECMA) standards before becoming an ISO/IEC standard, by a procedure called Fast-Track.

The first NFC-compatible mobile phones were distributed by Samsung and Nokia in 2005. In the same year the first field trials in payment with NFC started in France . The world's first commercial rollout of NFC was in Austria. Mobilkom Austria, OEBB and Wiener Linemen placed about 450 NFC tags at vending machines to support the customer, in buying tickets for the railway and underground via SMS. For the near future, commercial use of NFC technology is expected to increase. This is due to the fact that three smart phone operating system / device manufacturers \Apple (I Phone), Google (Android) and RIM (Blackberry) have announced plans to include NFC in their next products. Additionally, MasterCard, an international debit card company, is about to start its Pay Pass, an NFC based payment solution.

The most important NFC standards, in relation to the operation modes, are ECMA-340: Near Field Communication Interface and Protocol (NFCIP-1) and ECMA-352: Near Field Communication Interface and Protocol - 2 (NFCIP-2.NFCIP-1 combines the two RFID communication protocols: MIFARE (ISO/IEC14443 Type A [31]) and Felecia (JIS X 6319-4), and extends them with new communicaion possibilities and a new transport protocol. NFCIP-2 combines NFC with the functionality of RFID readers. This way NFC is compatible with most RFID devices .

2.PROPOSEDSYSTEM

In this method nfc tag structure gives security with symmetric asymmetric cryptography. The major point is the word explained total real word rfid system. This having all components for manufacture .many output will taken due to making work. in its place of by means of a finite-state machine-based controlling. The cause lies in the information that the controller can be just reused by many hardware elements, like tha CU or the RFID FL that would need extra area while improved as personality hardware modules.

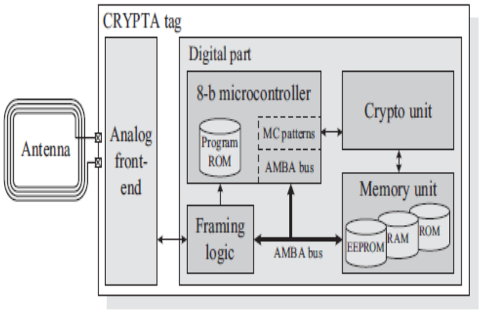


Figure 2.1 Block diagram of proposed system

This topic provides about crypta tag as well it major elements .it explained performance that will given by atag .

An indication of the structural design of the CRYPTA tag is given in Fig.3.1. The tag mostly contains of an analog front end and a digital part. The analog front-end is linked to an antenna and is liable for demodulating and modulating data,obtaining the power supply, and given that a stable clock signal and a reset signal. Attached to the analog front-end is the digital part, which processes the received , performs the requested events, and making ready of data to tag .

2.1 FRAMING LOGIC

The framing logic nothing but handling the basic tag functuality and it is aserial to parallel interface. Fig. 3 shows tha structural vision with such blocke are rx and tx control uunit amba interface. The Rx Tx unit is the interface between the serial data signals of the analog front-end and the parallel data signals of the control unit. as well, the Rx Tx unit taking the a clock signal from the analog front-end, which is used to additional bit. a bit-clock signal that will giving to the microcontroller and the additional components of the tag's digital part.the data rate in the default 106 kb/s, which gives bit-clock signal had a frequency of 106 kHz. The incoming signal can be sample by the rx tx unit, an information from the unit of control is appended by checksum, encoded, and transfomred bit-by-bit to the analog front-end. This unit is also liable for correct timing of the tag response, this is wanted to the sendin time slot.

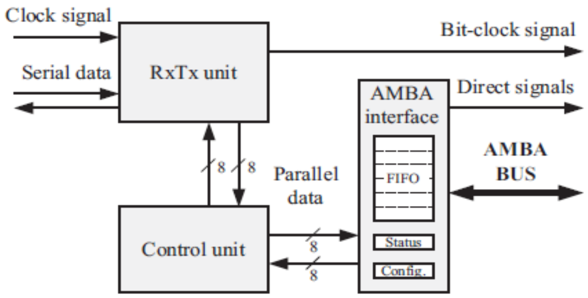


Figure 2.2 Basic blocks of Framing logic

3.Data path of the CU supporting ECDSA, AES, and SHA-1.

Functional blocks . The mold invites us to vary dissimilar parameters similar to the data path size. Each practical block of the form counts the numeral of needed clock cycles so that the implementation time of the realization can be roughly expected for given clock frequency. therefore, the calculation of ECDSA would want more than a few seconds while using a clock frequency of 1 MHz For a 16-b data size, we expected the computation to take about 0.8 s, or of 32 b and more, the expected execution time is concentrated to only a few hundred milliseconds or lower . In all-purpose, the earlier the realization, huge the range of probable RFID applications. whereas present re exist the applications anywhere long answer times be satisfactory, verification of goods in logistics or in admission control. though, selecting a better information breadth wants further hardware property still however it can procedure the operations a great deal earlier. The dominant part is the hardware multiplier. We so implemented and synthesized dissimilar hardware multipliers and compared the area supplies. It represents that if the volume of the data path is twise , the necessary area for the multiplier is amplified by a factor of 4. Such 8-b multiplier wants 380 GEs, 16-b multiplier wants 1600 GEs, and 32-b multiplier wants 6700 GEs. so that 16 bit multiplier , is a good tradeoff between area and required speed.

In figure two divided ALUs for ECDSA plus AES whereby in the ECDSA part, 16 bit multiplier and two 40-b adders construct the middle components. For ECDSA improved

also, we included the rational operations such as AND, OR, XOR in the ECDSA data path, which are too the major operations in SHA-1. ECDSA can use again these operations The ALU in the AES mostly contains of an AES S-box as well Mix Columns multiplier. This structural design extracted low-power AES completion of
In count, we determined to divide the AES data path in to the 2 (8-b) operations. It can invites us

to use again the residual 8 b to implement countermeasures next to completion attacks. In fact, we implemented copy AES rounds and shuffling of bytes in the AES state

4 ALGORITHMS

4.1 AES(ADVANCED ENCRYPTION STANDARD)

All of the cryptographic algorithms we have looked at so far have some problem. The earlier ciphers can be broken with ease on modern computation systems. The DES algorithm was broken in 1998 using a system that cost about $250,000. It was also far too slow in software as it was developed for mid-1970's hardware and its no giving proficient software programme.. 3ple DES on the other hand, has three times as many rounds as DES and correspondingly slower. As well as this, the 64 bit block size of triple DES and DES is not very efficient and is questionable when it comes to security. What was required was a brand new encryption algorithm. One that would be resistant to all known attacks. The (NIST) wanted to help in the creation of a new standard. However, because of the controversy that went with the DES algorithm, and the years of some branches of the U.S. government trying everything they could to hinder deployment of secure cryptography this was likely to raise strong skepticism. The problem was that NIST did actually wanton help create a new excellent encryption standard but they couldn't get involved directly. Unfortunately they were really the only ones with the technical reputation and resources to the lead the effort.

4.1.1 AES CIPHER

Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption. However, AES is quite different from DES in a number of ways. The algorithm Randal allows for a variety of block and key sizes and not just the 64 and 56 bits of DES' block and key size. The block and key can in fact be chosen independently from 128, 160, 192, 224, 256 bits and need not be the same. However, theAES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES- 256 respectively. so like this type of dis simillaries also AES differ from DES but its not festiel body. In this halves are swappwd to modify the half of the data block was utilized foe another of the data block. in it substitution and permutations are done to the entire data block.

4.1.2 INNER WORKINGS OF A ROUND

The add rond key is the starting key. stage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of its counterpart in the encryption algorithm. The four stages are as follows:

1. Substitute bytes
2. Shift rows
3. Mix Columns
4. Add Round Key

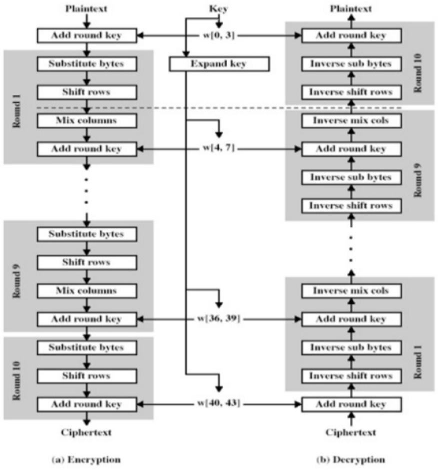


Figure 4.1 Overall structure of the AES algorithm

4.1.3 SUBSTITUTE BYTES

This stage (called as Sub Bytes) easily it can be use s box which has 16x16 matrix of bytes. It contain all combinations for 8 bit sequences. (28 = 16 × 16 = 256).any how s box is used for this algorithms.. The designers of Randal showed how it will do different the s-boxes in DES for which no motivation was given. We will not be concerned here how the s-boxes are made up and can simply take them as table lookups. Again this matrix can be operated on only known state encryption upto entire method. We will be concerned with how this matrix is affected in each round. For this particular.

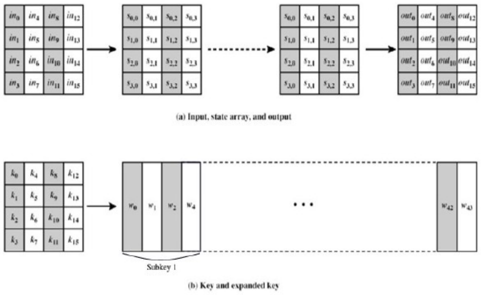


Table 4.2 Data structures in the AES algorithm

The following was given tha round each byte is mached to new byte.the last left side nibble of byte was utilized for shown a specific row for sbox and the show a right most nibble of coloum. To understand the given byte {95} which denotes hex values in fips fub.selects row 9 column 5 whose turns out to having the {2A}. it will be utilized to update **state** matrix.

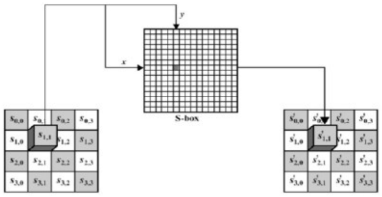


Table 4.4 Substitute Bytes Stage of the AES algorithm

In this s box will be used that is iverse sbox. transformation (known as Inv Sub Bytes) In it method what is for selecting value 2a the take the value is s box for manipulating the known cryptanalytic attakes. Importantly the Randal developers sought a design this has a low correlation among i/p and o/p bits the it could not be described of its property as a simple mathematical purpose of the input. In count, actually s box cannot contains complimentary values. This s-box should inverse while description will possible simply it should not be its inverse itself . Table 4.1.3(C) shows 2 s-boxes and it can be established.

4.1.4 SHIFT ROW TRANSFORMATION

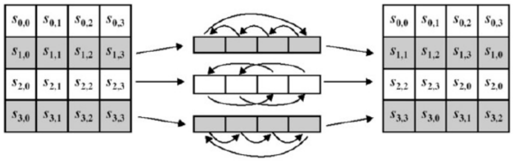
This stage (known as Shift Rows) is shown in figure 4.1.4(a). This is a simple permutation an nothing more. It works as follow:

- in the state first row is not changed.

• In the circular method 2nd row is shifted one byte to the left side.

• again The 3rd row is shifted two bytes to the left in a same to the abobe manner.

- The fourth row is shifted 3 bytes to the left in a circular manner.


$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,1}$ $s_{1,2}$ $s_{1,3}$ $s_{1,0}$
$s_{2,2}$ $s_{2,3}$ $s_{2,0}$ $s_{2,0}$
$s_{3,3}$ $s_{3,0}$ $s_{3,1}$ $s_{3,2}$

.

Table 4.4 Shift Rows stage.

It is also called inverse shift transformation .it can be done by circular shift in opposite direction foe each last 3 rows. (the first row was unaltered to begin with).it can not visit to do a large amount but while we are think that in what way the bytes are ordered in the state. Then it will be seen to impact. Note that state is denoted as an aarray of 4 byte coloum., i.e. the first column actually given by bytes 1, 2, 3 and 4. A one byte shift is so that a linear distance of 4 bytes. The transformation also given that 4 bytes of one column are spread out t o4 dissimilar columns.

4.5 MIX COLUMN TRANSFORMATION

This stage (called as Mix Column) was actually a substitution but it done utilization of arithmetic gf(28). every column is operated on independently. Every byte in the coloum is mached a original value that is a function of all4 bytes in the column. The alteration can be resolute by the following matrix growth on **state.** In the products matrix every element in the product matrix is equals to the addition of product of row and coloun. So that the personality summations and multiplications are performed in GF(28). The Mix Columns interchange of a column j (0 _ j _ 3) of **state** can be expressed as;

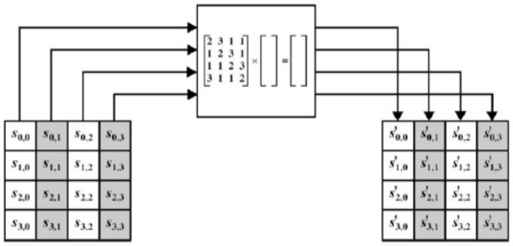

2 3 1 1
1 2 3 1
1 1 2 3
3 1 1 2
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Table 4.5 Mix Columns stage.

4.1.6 AES KEY EXPANSION

The AES key extension algorithm takes as input a four-word key and gives a linear collection of 44 words each rounds uses four these words. Given in following figure above.. every one word contains 32 bytes which means every sub key is 128 bits extensive.

The key is derivative into the first 4 words of the extended key. The remainder of the extended key is full in four words at a time. Each extra word **w**[i] based on the instantly earlier word, the 4 positions will back. The xor gate used to the in 3 out fo 4 cases.. For a word whose situation in the **w** collection is a many of 4, a further complex function is used. Figure 7.8 illustrates the invention of the first eight words of the extended key using the symbol g to correspond to that complex function. The function g contain of the subsequent sub functions:

1. **Rot Word** .proceed a 1 byte left shift method on a circular manner. It will get an input word [b0, b1, b2, b3] is changed into [b1, b2, b3, b0].
2. **Sub Word** performs a byte replacement on every byte of its input word, by means of the s-box described previous.
3. The result of steps 1 and 2 is XOR e d with round constant, R con[j].

The rightmost of 3 bytes oftenly zeros.which is known as word. So that the xor will proceed on only leftmost bytes of word.

The round regular is dissimilar for every round and is definite as R con[j] =(RC[J], 0,0,0), with RC[1]= 1, RC[j]= 2• RC[j −1] and with increase defined over the field GF.

The key extension was planned to be opposed to to recognized cryptanalytic attacks. Still eliminates the symmetry or similarity, between the method in which round keys are produced in dissimilar rounds.

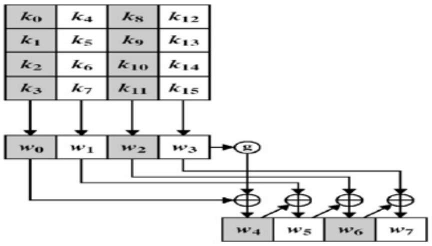


Table 4.6AES key expansion.

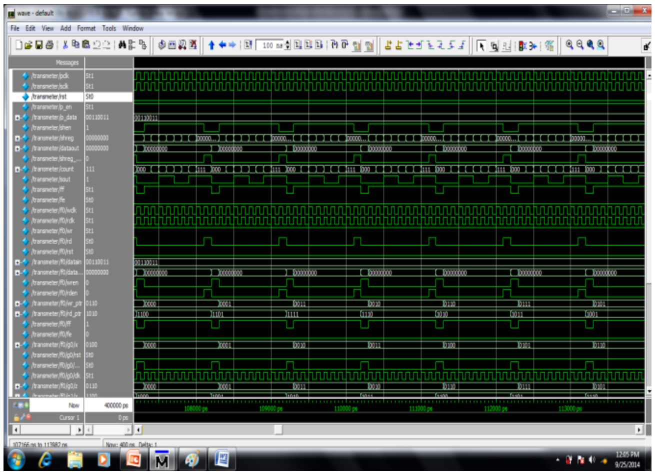
under Figure give a review of every of the rounds. The Shift Rows column is depicted now as a linear shift which gives a improved idea how this part helps in the encryption.

5.ECDSA(ELLIPTICAL CURVE DIGITAL SIGNATURE ALGORITHM)

The Digital Signature Algorithm (DSA) was exacting in a U.S (FIPS) called the Digital Signature Standard .Its security is depends on the computational intractability of the dissimilar type of various methods problems in 1st order subgroups.. Elliptic curve cryptosystems (ECC). They can be showed as elliptic curve analogues of the elder discrete logarithm (DL) cryptosystems in whose the other group altered with help of group of points in the curve. in excess of a programmed field. The arithmetical source for the security of elliptic curve cryptosystems is the computational intractability of the elliptic curve discrete logarithm problem Since the this method come into view to be considerably harder than the DLP, the strong key bit is very better in the given curve than tyhhe other various algorithms so , slighter parameters will be will be utilized than the descret algorithms. but with corresponding levels of security. The recompense that can be gained from slighter parameters contain speed and smaller keys and values. These compensation are especially significant in asusually when proceed in power saved space b/w are the ECDSA which is same to the DSA.

6.SIMULATION RESULTS &SYNTHESIS REPORT

6.1 SIMULATION RESULTS

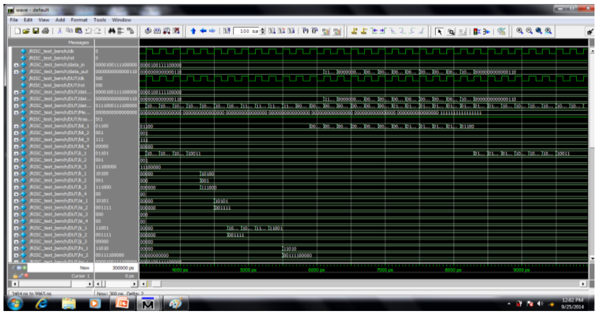


```
/transmeter/pclk          St1
/transmeter/sclk          St1
/transmeter/rst           St0
/transmeter/p_en          St1
/transmeter/p_data        00110011
/transmeter/shen          1
/transmeter/shreg         00000000
/transmeter/dataout       00000000
/transmeter/shreg_...     0
/transmeter/count         111
/transmeter/sout          1
/transmeter/ff            St1
/transmeter/fe            St0
/transmeter/f0/wclk       St1
/transmeter/f0/rclk       St1
/transmeter/f0/wr         St1
/transmeter/f0/rd         St0
/transmeter/f0/rst        St0
/transmeter/f0/datain     00110011
/transmeter/f0/data...    00000000
/transmeter/f0/wren       0
/transmeter/f0/rden       0
/transmeter/f0/wr_ptr     0110
/transmeter/f0/rd_ptr     1010
/transmeter/f0/ff         1
/transmeter/f0/fe         0
/transmeter/f0/g0/x       0100
/transmeter/f0/g0/rst     St0
/transmeter/f0/g0/...     St0
/transmeter/f0/g0/clk     St1
/transmeter/f0/g0/z       0110
Now                       400000 ps
Cursor 1                  0 ps
107166 ps to 113982 ps    Now: 400 ps  Delta: 1
```

Figure 6.1 UART simulation results

In this the serial data and clock signals are applied to the UART. It produced bit-clock signal and give to the parallel data. This parallel data applied to control unit . the control unit was control to the operations of the AMBA interface and also shows the status of the FIFO.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 07, July 2015
Available at http://internationaljournalofresearch.org



.

Figure 6.2 Micro controller Simulation Results

The framing logic output applied to the micro controller. It performs to the inside to make 31 operations, after the micro controller produced the output. This output is called encrypted data.

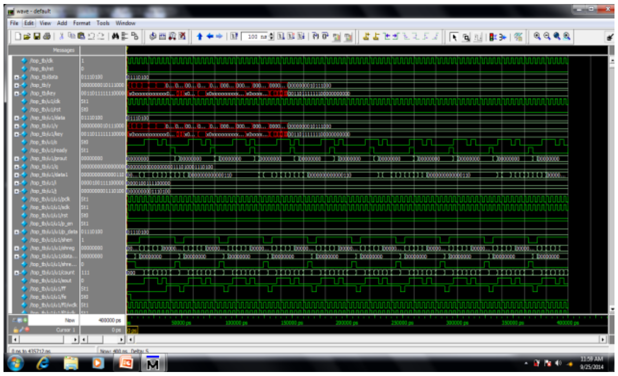


Figure 6.3 simulation results for key generation

6.2 RTLSCHEMATIC

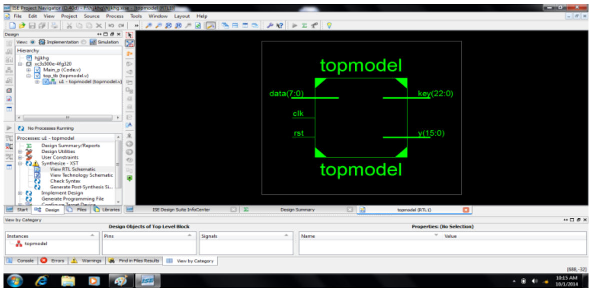


Figure 6.4 Top Level Circuit

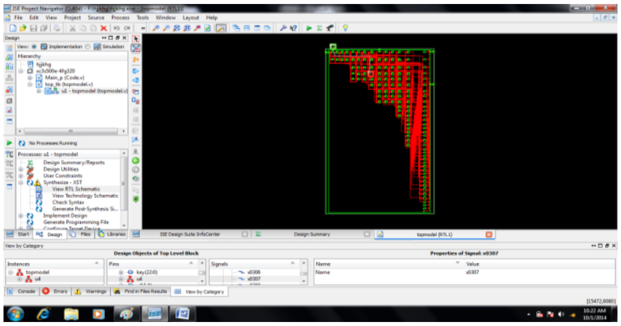


Figure 6.5 RTL Schematic diagram

6.3 TECHNOLOGY SCHEMATIC

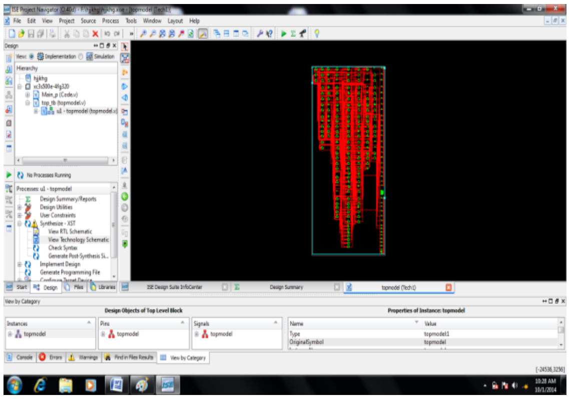


Fig6.6 Technology Schematic

CONCLUSION AND FUTURE SCOPE

In this scheme, we offered a flexible NFC-tag structural design that gives improved protection abilities using both symmetric and asymmetric cryptography. As a chief contribution, the work described an complete “real-world” RFID system, counting total hardware elements are essential to the predefined fabrication. throughout the work, anumber of outcomes were obtained. First, our aim showed that important resources will be stored with applying a microcontroller-based method as an alternative of using a fsm –with controlling. The starting point lies in the truth that the controller can be mostly again used by numerous hardware apparatus, such as the CU or the RFID FL that will require. additionaly area while implemented as independent hardware design. For example, AES encryption and decryption has been realized with an area above your head of only 2387 GEs, which is lower than existing low-area AES developments.additionally, SHA-1 needs only 889 GEs because of reusing available memory and microcontroller components of the whole system. Then to these outcomes, we establish that it is encouraging to reuse the microcontroller for RFID protocol handling, 4. This can be completely realized as a micro program, which decrease additional chip-area necessities while growing flexibility and assembly-based completion convenience. Finally, we virtually proved our design by manufacturing the system as a prototyping sample that demonstrates the possibility of a full-blow RFID/NFC tag supporting ISO/IEC 14443A layer 1–4, NFC Forum Type-4 features (including NDEF support), a flexible (programmable) 8-b microcontroller, memory (RAM, ROM, and EEPROM), analog frontend, and well-built cryptography (ECDSA and AES) for less than 50 kGEs.

FUTURESCOPE

In the upcoming, we sketch to further study our design concerning improved performance attacks, like as side channel study and fault attacks. additionally, we sketch to implement other demo applications to confirm the applicability of our tag in dissimilar security-related scenarios.

REFERENCES

[1] M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, “Strong authentication for RFID systems using the AES algorithm,” in Proc. CHES, vol. 3156.Aug. 2013, pp. 357–370.

[3] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, “Public-key cryptography for RFID-tags,” in Proc. RFIDsec, 2011, pp. 1–16.

[4] P. Tuyls and L. Batina, “RFID-tags for anti-counterfeiting,” in Topics in Cryptology, vol. 3860, D. Pointcheval, Ed. New York: Springer-Verlag, 2010, pp. 115–131

.

[5] NFC Forum Type 4 Tag Operation - Technical Specification. (2009, Mar.) [Online]. Available: http://www.nfc-forum.org/specs

[6] Identification Cards - Contactless Integrated Circuit(s) Cards – Proximity Cards - Part 3: Initialization and Anti collision, ISO/IEC Standard 14443-3, 2008.

[[8] Information Technology - Identification Cards - Integrated Circuit(s) Cards with Contacts - Part 4: Inter industry Commands for Interchange, ISO/IEC Standard 7816-4, 2007

[9] National Institute of Standards and Technology. (2006, Nov.). FIPS-197: Advanced Encryption Gaithersburg, MD [Online]. Available http://www.itl.nist.gov/fipspubs/

[10] National Institute of Standards and Technology. (2006). FIPS- 186-3: Digital Signature Standard (DSS), [Online]. Available: http://www.itl.nist.gov/fipspubs/

[11] T. Plos and M. Feldhofer, “Hardware implementation of a flexible tag Plat form for passive RFID devices,” in Proc. 14th Euro

micro Conf. Digit.Syst. Design, Aug. 2006, pp. 293–300.

[12] Infineon Technologies AG. (2003). Security and Chip Card ICs SLE 88CFX4000P, Neubiberg, Germany [Online]. line.cn/iol/datasheet/sle88cfx4000p_1310434.pdf

[13] J. Großschädl, "A bit-serial unified multiplier architecture for finite fields GF(p) and GF(2m)," in Proc. CHES, vol. 2162. May 2001, pp. 202–219.

[14] D. Hein, J. Wolkerstorfer, and N. Felber, "ECC is ready for RFID—a proof in silicon," in Selected Areas in Cryptography. Berlin, Germany: Springer-Verlag, Sep. 2001, pp. 401–413.