International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

RSA Cryptosystem Using Verilog

Deepak Mehra[1], Dr. Neelam Srivastava[2]

[1] Institute of Engineering and Technology, Lucknow (UP), India

[2] Professor, Department of Electronics Engineering, Institute of Engineering and Technology, Lucknow (UP), India

Abstract: ***Cryptosystem is a system which is used for network security for data transmission. By using this technique we can send any data from one place to another place and no unauthorized person can access or misuse this data. So this is a secure data transmission technique. There are many types of algorithms may be used according to user. In past time the user encodes the text data manually and then authorized person decode the data manually so it was much time taking and also security level was much low but there was no security for images and video. So in 1977*** *Ron Rivest, Adi Shamir, and Len Adleman introduce a new technique that is called cryptosystem or cryptography.* ***In this implementation includes three parts: key generation, encryption and decryption process. The key generation stage aims to generate a pair of public key and private key, and then the private key will be distributed to receiver according to certain key distribution schemes. We use Verilog to design these modules using Verilog HDL and synthesize the design with the help of Xilinx and Isim simulator.***

Keywords: Xilinx, Isim simulator. Cryptosystem, Decryption, Encryption, Key Generation, Modular Exponentiation, Modular Multiplication, RSA, Verilog.

1. Introduction

This paper proposes the hardware implementation of RSA encryption/decryption algorithm using Xilinx and Isim simulator. Cryptosystem is a system which is used for network security for data transmission. First ever in 1977 Ron Rivest, Adi Shamir, and Len Adleman introduce this technique so based on the scientist name its name is RSA cryptosystem. RSA is one of the first practicable public - key cryptosystems and is widely used for secure data transmission.Data communication uses RSA for key exchange. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. RSA is widely used for securing sensitive data, particularly when being sent over an insecure network such as internet. The cipher text can be decrypted at receiver side by RSA secret key.

The RSA algorithm is indeed among the strongest, but can it withstand anything? Certainly nothing can withstand the test of time. In fact, no encryption technique is even perfectly secure from an attack by a realistic cryptanalyst. Methods such as brute-force are simple but lengthy and may crack a message, but not likely an entire encryption scheme.

We must also consider a probabilistic approach, meaning there's always a chance someone may get the \one key out of a million". So far, we don't know how to prove whether an encryption scheme is unbreakable. Despite years of attempts, no one has been known to crack either algorithm. Such a resistance to attack makes RSA secure in practice.

To show that RSA is secure, we will consider how a cryptanalyst may try to obtain the decryption key from the public encryption key, and not how an intruder may attempt to steal" the decryption key. This should be taken care of as one would protect their money, through physical security methods.

These are simulated in Xilinx and hardware is synthesized using RTL Compiler. In this a third party generates a pair of public key and private key . Public key is distributed to transmitter and private key distributed to receiver. Generally public key and private key both are related to each other but both are different.[1,2,3,5,10,12]

2. The RSA key generation algorithm

Step 1: First ever we generate two prime numbers.
Prime no. those no. which are divisible by either by one or by self e.g. 2, 5,7,11 etc. These prime no. can be generate randomly but these two no. should not be equal.

Let two prime no. p and q. And $p \neq q$
e.g. p= 2and q= 5

Step 2: Calculate the multiplication of two prime numbers p and q and we get the value of n.

$$n = p \times q$$
$$n= 2\times5=10$$

Step 3: Calculate $\phi(n) =(p-1) \times (q-1)$

$$\phi(n) =1\times4 = 4$$

Step 4: Select 'e' such that 'e' is relatively prime to $\phi(n) = 4$ or GCD(e, $\phi(n)$) = 1 and less than $\phi(n)$. So here we choose the value of 'e' is 3. Because 3 is prime no. and also exist between 1 and 4.

Step 5: In this step we determine the value of 'd' Such that 'de = 1 mod $\phi(n)$' or 'de mod $\phi(n)$ = 1'. It means that we already know the value 'e'.and we have to select the value 'd' in such manner that above condition should be satisfied.
e.g. Here 'e' = 3 and $\phi(n)$ = 4 condition is 'de mod $\phi(n)$ = 1'. Divide the value 'de' by $\phi(n)$ and remainder should be 1. So choose d = 3. If'd' = 3 and 'e' = 3 then 'de' = 9. Divide 9 by 4 and get remainder 1.

Finally we get the value of ‘n’,’e’ and ’d’.In this encryption key will be (e,n) and decryption key (d,n). Encryption and decryption have the following form, for some plaintext block M and cipher text

C = M^e (mod n). (Encryption)

Let, Massage(M) = 7;

C = 7^3 (mod 10)

C = 3

By using the formula cipher text again gives the massage text.

M = C^d(mod n). (decryption)

= 3^3(mod10)

= 7

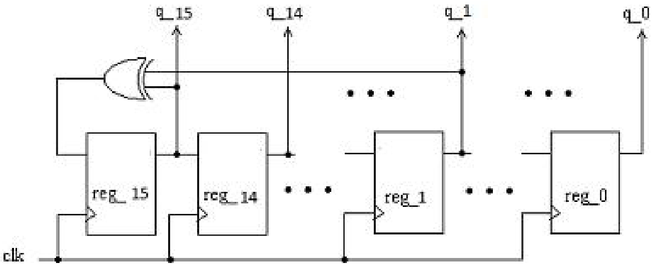
So here decrypt the signal and we get result 7 which was the massage signal we have given.[2,3,4]

3. Implementation Process of RSA Cryptosystem

3.1. Random Number Generator

For implement the RSA cryptosystem first ever we generate random number. To generate Random Number we use Linear Feedback Shift Register (LFSR) linear feedback shift register can generate a (2n-1)-bit long random sequence without repeating. In this we have use 16-bit LFSR.

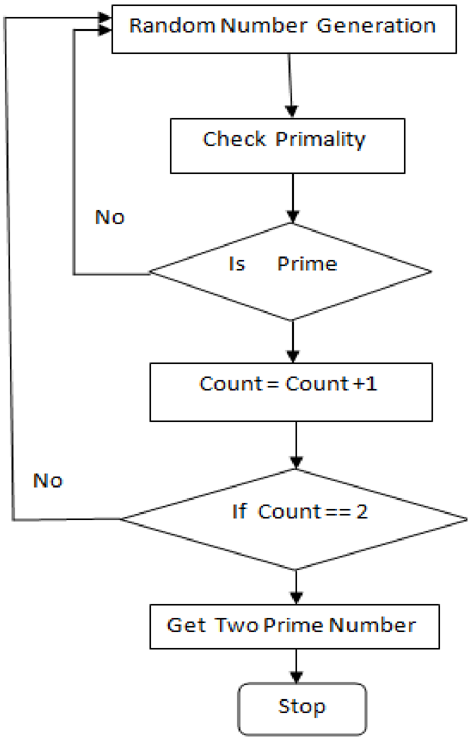
In LFSR There is 16 registers and one XOR gate it perform XOR operation between 15th bit and first bit and give the feedback to 15th register and shift the bit for every clock is applied. The fig. of LFSR is shown below.[2,3,6,7]



Structure of the 16-bit LFSR

3.2. Primality tester

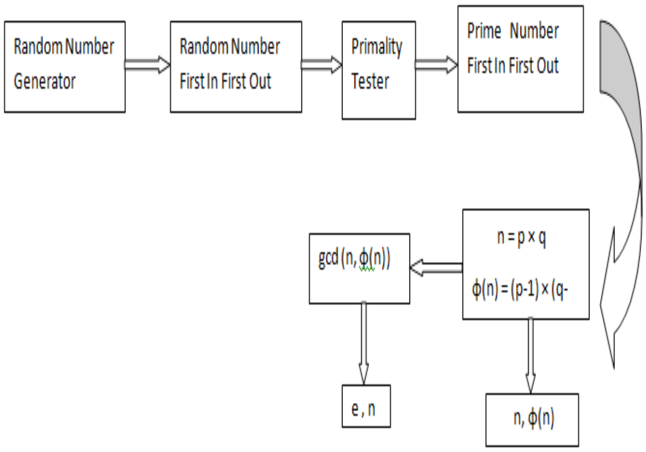
The basic purpose of Primality tester is that to test the random number that it is prime or not. First LFSR generate the number randomly in this all number takes place. But here we required only prime so after LFSR Primality tester is required.



Structure of the Primality tester

The process is stopped as soon as two prime numbers are generated. Flowchart for Random number Generator is shown above.[2,3,8,9]

3.3 Complete RSA key generation system



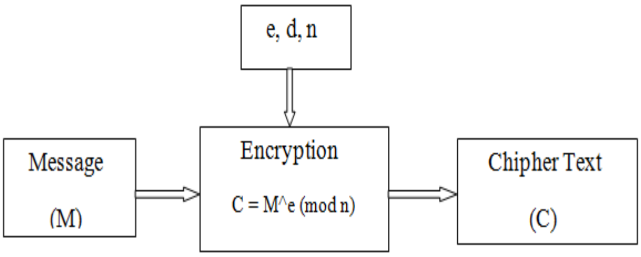
Block diagram of RSA key generation system

As we get the value of two prime numbers we will get the value of n and ϕ(n).And by using this value we will get the value of ‘e’ and ‘d’ as the method explained above. So encryption key is (e,n) and decryption key (d,n).[1,2,3]

3.4 Encryption Process

When we know the value of e, n and d then we implement a verilog program in which a message signal gives as a input then cipher text comes out as a output using the formula [1, 2, 3]

C = M^e (mod n).



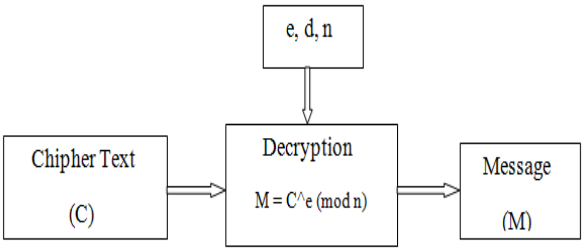
Block diagrm of Encryption

Here 'M' is the message signal
'e' is encrypt key
'n' is the multiplication of two prime numbers.

Let, Message(M) = 7, 'e' = 3 and 'n' = '10'
C = 7^3 (mod 21)
C = 3 (cipher text)

3.5 Decryption Process

In decryption the process is same as the encryption in this process only we use the value of 'd' in place of 'e' .In this the cipher text is given as input in modular exponential and we get same message as the output which we have applied as input in the encryption.[1,2,3]



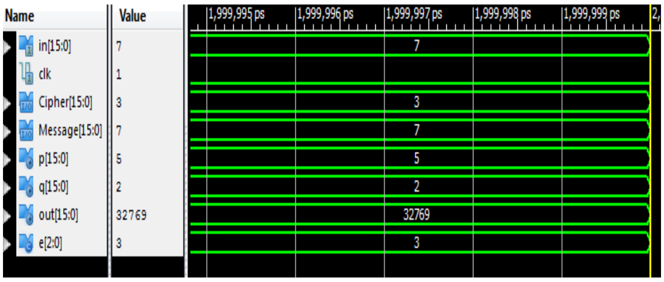
The RSA decryption structure

M = C^d(mod n). (decryption)
= 3^3(mod10)
= 7

So here decrypt the signal and we get result 7 which was the message signal we have given.

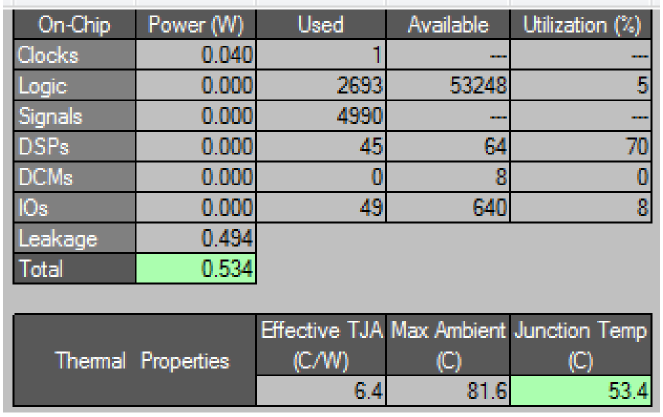
4. Simulation Result

We design the VERILOG code for RSA cryptosystem. As we know that VERILOG is a hardware descriptive language.
We use Xilinx software and I-Sim simulator to simulate the program and get result. We apply input 7 we get cipher text 3 and output again get 7 which message signal we have applied.



Simulated Waveform

5. Power Analyzer



On-Chip	Power (W)	Used	Available	Utilization (%)
Clocks	0.040	1	---	---
Logic	0.000	2693	53248	5
Signals	0.000	4990	---	---
DSPs	0.000	45	64	70
DCMs	0.000	0	8	0
IOs	0.000	49	640	8
Leakage	0.494			
Total	0.534			

Thermal Properties	Effective TJA (C/W)	Max Ambient (C)	Junction Temp (C)
	6.4	81.6	53.4

Power Consumption Report
Here we can see that power consumption of our device is 0.6 watts. We are trying to reduce power.

6. Conclusion

A cryptosystem is simply an algorithm which converts the input data plaintext into something cipher text and converts the unrecognizable data back to its original form. In this implementation a 16-bit RSA circuit is made using Verilog. The basic RSA circuit including Key generation, data encryption and data decryption. We are using here VERILOG hardware descriptive language to enhance the security. By using verilog a million of gates can be design on a small chip and power consumption is very low. The software we use Xilinx and I-sim simulator is used to simulate the design. Here security level is high because here 16- bit LFSR is used to generate random number. This design assurance that the communicating entity is the one claimed, prevention of the unauthorized use of a resource, protection of data from unauthorized disclosure and assurance that data received is as sent by an authorized entity.So finally The RSA cryptosystem is a technique by using which we can send data to any one by secure way and we are trying to do best to improve this technology.

References

[1] Chiranth E Chakravarthy H.Y.A, Nagamohanareddy P, Umesh T.H, Chethan Kumar M, " Implementation of RSA Cryptosystem Using Verilog', International Journal of Scientific & Engineering Research Volume 2, Issue 5, May-2011.

[2] R.L .Ri vest, A. Sha mir , and L . Adl eman, "A Method for Obtaining Digital Signatures and Public- Key Cryptosystems", communicatios of the ACM 2 1 (1998).

[3] William Stallings, "Cryptography and Network Security Prentice –Hall of India private limited, Third Edition (2004).

[4] Neal Koblitz, "A Course in Number Theory and Cryptography", Springer, Second Edition 2000.

[5] Implementing the Rivest, Shamir, Adleman cryptograph algorithm on the Motorola 56300 family of digital signal processors.

[6] Ridha Ghayoula, E. I. Amjed H l aoui, Talel Korkobi, Mbarek Traii, Hichem T rabelsi,"FPGA Implementation Of RSA Cryptosystem", International Journal of Engineering and Applied Sciences 2 : 3 2006.

[7] Tzong - Sun Wu, Han -Yu Lin," Secure Convertible Authenticated Encryption Scheme Based on RSA ", Infor matica 3 3 (2009) 4 8 1 -486.

[8] Guilherme Perin, Daniel Gomes Mesquita, and Jo-Ao Baptista Martins,"Montgomery Modular Multiplication On Reconfigurable Hardware : Systolicversu Multiplexed Implementation ", Hindawi Publishing Corporation International Journal of Reconfigurabl Computi ng Volume (2 0 1 1)

[9] Chung -Hsien Wu, Jin-Hua Hong and Cheng-Wen Wu, VLSI Design of RSA Cryptosystem Based on the Chinese Remainder Theorem ", Journal of Information Science and Engineering 1 7,967 - 980 (2001).

[10] Md. AI i -AI-Mamun, Mohammad Motaharul I slam, S . M. Mashihure Romman and A.H. Salah Uddin Ahmad, " Performance Evaluation of Several Efficient RSA Variants", IJC SN S International Journal of Computer Science and Network Security, 8No.7, July (2008).

[11] Ramzi A. Haraty, N . EI -Kassar and Bilal Shibaro, "A Comparative Study of RSA Based Digital Signature Algorithms ", Journal of Mathematics and Statistics (1) : 3 54-3 5 9, 2006.

[12] Yi-Shiung Yeh, Ti ng-Yu Huang, Han-Yu Lin and y u-Hao Chang, "A Study on Parallel RSA Factorization", Journal of Computer s, vol . 4, no. 2, February 2009.

[13] Public-Key Cryptography and the RSA Algorithm by Avi Kak (kak@purdue.edu) April 22, 2015.

Author Profile

Deepak Mehra received the B.Tech degree in Electronics and Communication Engineering from Bundelkhand Institute of Engineering and Technology, Jhansi (UP) in 2010 and pursuing M.Tech degree in Micro-Electronics in Institute of Engineering and Technology, Lucknow(UP).

Dr. Neelam Srivastava is working as a professor in Institute of Engineering and Technology, Lucknow(UP). She received the B. E. degree in Electronics Engineering from M. M. M. Engineering College, Gorakhpur in 1985, M.Tech degree Microwaves from Institute of Technology, B.H.U, Varanasi and Ph.D in optical communication from Lucknow University in 2004.