Improved Mask Protected DES using RSA Algorithm

S.Asha Latha[1], A.Sivabalan[2]
[1]*Research Scholar, Sathyabama University,Chennai- 600119*
[2]*Manager Research, NEC Mobile networks Excellence Centre, Chennai.*
asha_26_2001@yahoo.com, sivabalan.armugam@necindia.in

Abstract: The data encryption standard is a pioneering and farsighted standard which helped to set a new paradigm for encryption standards. But now DES is considered to be insecure for some application. Asymmetric mask protected DES is an advanced encryption method for effectively protecting the advanced DES. There are still probabilities to improve its security. This paper propose a method, which introduce a RSA key generation scheme in mask protected DES instead of plain key, which result in enhancement in the security of present asymmetric mask protected DES. We further propose a Vedic mathematical method of RSA implementation which reduce the complexity of computation in RSA block thereby resulting in reduced delay (four times)that improves the performance of overall system. The software implementation was performed using Xilinx 13.2 and Model-Sim was used for the simulation environment.

Keywords: cryptography, security, data confidentiality, RSA, DES, Vedic mathematics

I Introduction

Cryptography is usually referred to, as the study of securing information.The aim of cryptography is not to hide the existence of a message but it rather hides its meaning. Encryption is the process of converting plain text to cipher text. The process of converting cipher text back to plain text is called decryption[4],[7].There are two basic cryptographic techniques one in symmetric or private key cryptography and another is asymmetric key cryptography . Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break[9]. Most symmetric encryption schemes today are based on this structure. Although this is considered "strong" encryption, DES is one of the symmetric encryption algorithm, which is considered to be insecure now a days. Asymmetric mask protected DES is also a symmetric cryptography where an extra masking technique is used to increase the security of DES shown in fig 1 and fig 2. There are still probabilities to improve its security and efficiency. Here, a new method is introduced where in the already existing key generation scheme is replaced by RSA encryption. RSA prime factorization involved in it increases the security thus making it resistant to side channel attack such as correlation power analysis attacks and differential power analysis attack[2],[3]which is used to crack the plain text[10],[11]. Further Vedic mathematical calculations are involved to reduce the complexity of encryption in RSA block which further improves the efficiency of the proposed method[13].The rest of the paper is organized as follows. Section II describes the asymmetric mask protected DES, and Vedic Implementation. Section III describes the proposed improved encryption mechanism using RSA algorithm. Section IV describes the simulation environment and results. Section V contains conclusion and the future scope.

II. BACKGROUND

a. Asymmetric Mask Protected DES

The asymmetric mask protected DES is a data encryption standard where a masking technique is introduced in the normal DES algorithm[1]. Like most of the encryption schemes mask protected DES expects two inputs – the plain text to be encrypted and the secret key. The main idea in this method is to add different random numbers in the first, last and internal rounds. This method also has 16 rounds of operation similar to DES. Hence multiple mask operations added at different moments and locations helps to break the relation between power consumption and key thereby improving security.

b. Vedic Implementation

The RSA Algorithm is the most popular asymmetric key cryptographic algorithm.. The RSA Algorithm is based on the mathematical functions that are easy to find and multiply the large numbers together, but it is

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

extremely difficult to factor their product[5]. The public and private keys in RSA are based on very large numbers. To increase the computation speed with minimized hardware the Vedic mathematics [6]multiplication principle is used. These architectures are used to improve the speed of the RSA algorithm with reduced hardware[7],[8].

Mask Protected DES Encryption and Decryption:

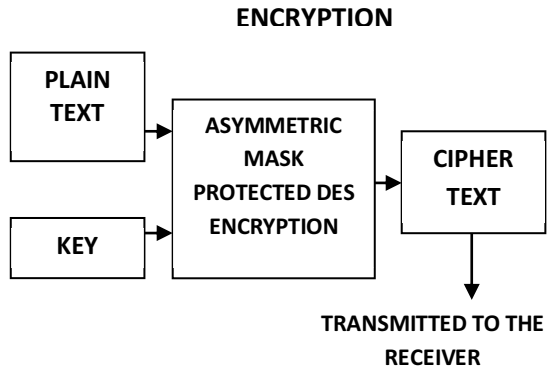

Fig 1. Mask protected DES Encryption

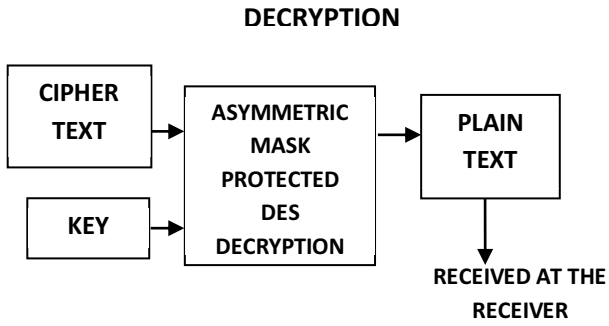

Fig 2. Mask Protected DES Decryption

III Improved Asymmetric Mask Protected DES

In the proposed system, instead of normal key generation of mask protected DES, RSA algorithm which is a asymmetric key algorithm is used. The advantage of asymmetric key is that it is secure from the middle attack unlike symmetric key. During the process of encryption, asymmetric mask protected DES encrypts the plain text to produce the cipher text.The key is encrypted using RSA at the sender side before transmitting it to the receiver shown in fig 3. Finally the combination of the key from RSA encryption and the cipher text from mask protected DES is sent out. At the receiver two cipher texts are obtained shown in fig 4. One is cipher text from asymmetric mask protected DES encryption and the other is the cipher key from the RSA encryption. The receiver decrypts the cipher key received from RSA encryption by their own private key. Then using the decrypted original key, the cipher text is decrypted. Finally the original plain text is received at the receiver end. This method ensures improved data confidentiality and integrity because of the deal protection of asymmetric mask protected DES algorithm and RSA algorithm, the data in transit is safe.

Improved Mask Protected RSA Encryption:

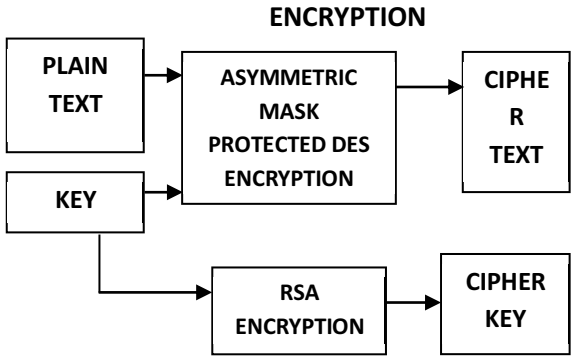

Fig 3.Improved Mask Protected RSA Encryption

Improved Mask Protected RSA Decryption:

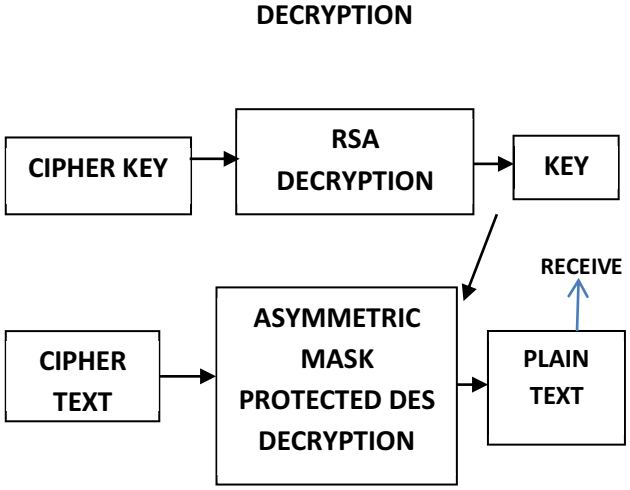

Fig 4.Improved Mask Protected RSA

DOI: 10.1051/matecconf/20166501005

On other hand, one has to accept the fact that securing always increases the complexity of an encryption procedure thereby consuming more power for encryption and decryption. Secondly this complexity reduces the speed of data processing thereby increasing the delay. Hence security as always compromised with speed and throughput performance to some extent in any encryption techniques. In the proposed method the existence of array multiplier is replaced by Vedic multiplier in the RSA block. This replacement produced four times reduced delay values when compared to the usual array multiplier used in RSA. To increase the computation speed, the multiplication principle of Vedic mathematics is used. And also “URDHVA-TIRYAKBHYAM” is the sutra (principle) which is used to compute the multiplication. The significance of this technique is that it computes the partial products in one step and avoids shifting operation which reduces the complexity of the algorithm and saves both the execution time and hardware. This ultimately improves the speed of RSA algorithm[13],[12]. Hence the secure dual protection of asymmetric mask protected DES and RSA is achieved with less complexity.

IV. Result and discussion

The proposed method is simulated using ModelSim 6.3 g and code in written in verilog using Xilinx. Fig.5 shows the encrypted output of proposed method. The input and output details are given below.

Plaintext -
00000000000100010010001000110011010001000101010101100110011101111

InputKey-
0000000100100010001101000101011000000000100100010001101000101011 0

Mask-0000000100100010001101000101011

Ciphertext-
1000100011100001101000101001100110010010001100100111010011000010

Cipherkey-
000000000000000000000000000000010000000000000000000000100110101000000000000000000000000010000110100000000000000000000000000011001010100000000000000000000000010000000000000000000000010011010100000000000000000000000000100001101000000000000000000000000110010101

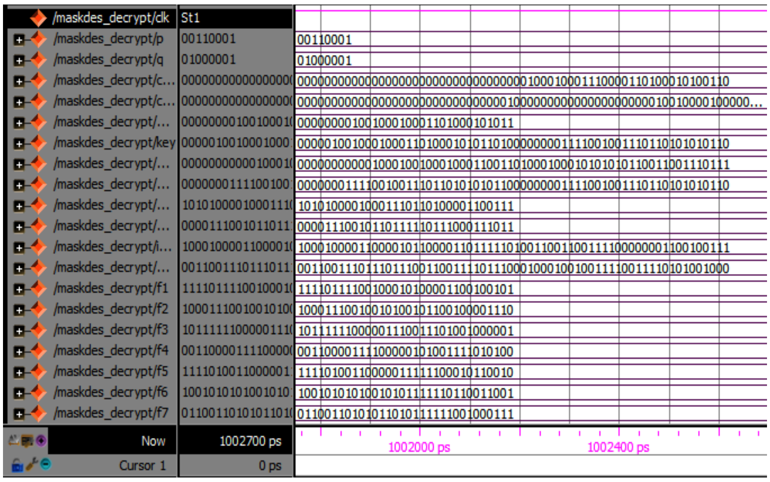

Fig.5 Encrypted output waveform for proposed system

Fig.6 shows the decrypted output of proposed method. The input and output details are given below.

Ciphertext-
1000100011100001101000101001100110010010001100100111010011000010

Cipherkey-
000000000000000000000000000000010000000000000000000000100110101000000000000000000000100001101000000000000000000000000000011001010100000000000000000000000000000100000000000000000000000100110101000000000000000000000000000010000110100000000000000000000000110010101

Mask-0000000100100010001101000101011

Plaintext-
00000000000100010010001000110011010001000101010101100110011101111

InputKey-
00000001001000100011010001010110000000001001000100011010001010110

Even if the attack sample is increased five times, the attacker still cannot gain the key when improved asymmetric masked DES using RSA is used. Hence the proposed method is resistant to differential power analysis attack and correlation power analysis attack.

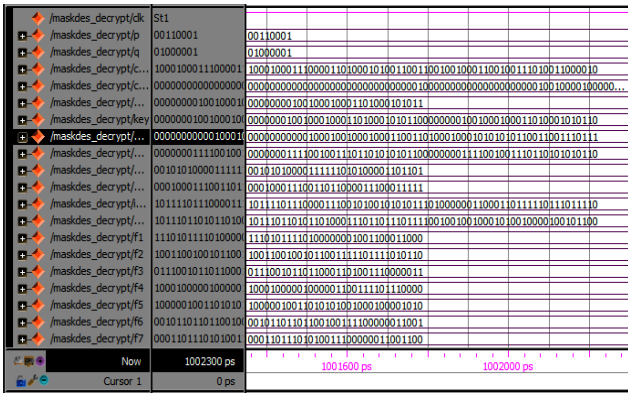

Fig.6 Decrypted waveform for proposed system

V. CONCLUSION

The improvedmask protected DES encryption mechanism using RSA algorithm is a full featured circuit including key generation, data encryption and data decryption. Each sub component and top module of the proposed encryption mechanism was implemented using verilog and was simulated using ModelSim which proved to be functionally correct. Dual security is achieved by the use of random numbers and RSA algorithm thus resistant to side channel attack. The complexity in the proposed system is reduced by using Vedic mathematical calculation which produced four times lesser delay values. Since the demand for higher levels of security is increasing the use of the proposed mechanism makes the entire algorithm difficult to crack. As a result, security is enhanced. The obtained Less delay values promotes high speed and low power consumption, thus promoting efficient hardware implementation on FPGAs. Future work can be carried out on cadence. The proposed method can also be implemented in Bluetooth technology and hybrid encryption. The work can also be extended to large bits such as 256 or 1024 or even longer and can be used in many applications where security is of major concern.

References:

1. Weiwei Shan Member IEEE “Evaluation of Correlation Power Analysis Resistance and Its Application on Asymmetric Mask Protected Data Encryption Standard Hardware”, IEEE Transaction on instrumentation and measurement, Vol. 62 No.10 (2013).
2. Akkar.M.L and Giraud .C (2001), “An implementation of DES and AES secure against some attacks”, in Proc. Cryptographic Hardware Embedded Syst, Paris, France, pp.309-318.
3. Weiwei Shan, Xin Chen, Bo Li, Peng Cao, Jie Li, Gugang Gao, and Longxing Shi (2013), “Evaluation of Correlation Power Analysis Resistance and Its Application on Asymmetric Mask Protected Data Encryption Standard Hardware”, IEEE Transactions on Instrumentation and Measurement, Vol. 62, No.10, pp.2716-2724.
4. WilliamStallings (2005), "Cryptography and Network Security Principles and Practices", Prentice Hall, November 16, pp.24-28, 56-83.
5. HimanshuThapliyal and M.B Srinivas, “VLSI Implementation of RSA Encryption System Using Ancient Indian Vedic Mathematics”, Center for VLSI and Embedded System Technologies, International Institute of Information Technology Hyderabad-500019, India.
6. Shamim Akhter, “VHDL Implementation of Fast NXN Multiplier Based on Vedic Mathematics”, Jaypee Institute of Information Technology, University, Noida, 201307 UP, INDIA, 2007 IEEE.
7. BehrouzAForouzan, DebdeepMukhopadhyay,”Cryptography and Network Security”, second edition, *Tata McGraw Hill Education Pvt Ltd*, 2008.
8. Nitish Aggarwal, KartikAsooja, SaurabhShekhar Verma, SapnaNegi,” An Improvement in the Restoring Division Algorithm”, IEEE 2009.
9. Sumit Vaidya, Deepak Dandekar, “Delay-Power Performance Comparison of multipliers in VLSI circuit design”, *International Journal of Computer Networks & Communications* (IJCNC), Vol.2, No.4, July 2010.
10. J. Wu, Y. Shi, and M. Choi, “Measurement and evaluation of power analysis attacks on asynchronous S-box,” *IEEE Trans. Instrum.Meas.* vol. 61, no. 10, pp.2765–2775, 2012.
11. J. Li, Y. Lv, H. Sun, and W. Shan, “A power analysis resistant DES cryptographic algorithm and its hardware design,” in *Proc. 3rd Int. Conf. Digit. Manuf. Autom.*, GuiLin, China, pp. 121–124, 2012.
12. Chiranth E, Chakravarthy H.V.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
13. Bhaskar, Ganapathi Hegde, P.R.Vaya, “Anefficient hardware model for RSA Encryption

system usingVedic mathematics", International Conference on Communication Technology and SystemDesign2011.