UNIVERSITI PUTRA MALAYSIA

HYBRID CRYPTOGRAPHY ALGORITHM TO IMPROVE SECURITY CLOUD STORAGE

INAM RAZZAQ ABD ALMOHSEN
GS45012

FSKTM 2017 4

HYBRID CRYPTOGRAPHY ALGORITHM TO IMPROVE SECURITY CLOUD STORAGE

By

INAM RAZZAQ ABD ALMOHSEN

GS45012

Thesis Submitted in Fulfillment of the Requirement for the master's degree of Computer Science and Information Technology/Specialization: Distributed computing

Faculty of Computer Science and Information Technology

University Putra Malaysia

June, 2017

APPROVAL

This thesis report is submitted to the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, and has been accepted as partial fulfillment of the requirements for the Master's degree of computer science/Distributed computing. The members of the Examination Committee are as follows:

_____

Supervisor
DR. MASNIDA HUSSIN
Dept. of Communication Technology and Network
Faculty of Computer Science & Information Technology
University Putra Malaysia (UPM) Serdang,
Selangor MALAYSIA

_____

Examiner
AP DR. ZURINA MOHD HANAPI

DEDICATION

To my Parents, Family and my husband

ACKNOWLEDGEMENTS

In the name of Allah the most Beneficent and the most Merciful, first and foremost, I would like to express gratitude to Allah Almighty, for endowing me the opportunity, patience and guidance to complete this thesis successfully.

Secondly, I owe my deepest gratitude to my supervisor, Dr. MASNIDA HUSSINfor her guidance and support. I would also express thanks to my examiner AP DR. ZURINA MOHD HANAPI for giving me the guidance and invaluable help.

I am also profoundly grateful to my colleagues and friends for their motivation and moral support, mostly when I become apprehensive about composing this thesis.

Finally, I would like to thank my family for their continuous supports throughout the process. Their advices and concerns have been the greatest inspiration for me to sail through the phases of stress in doing this thesis. Without their all-round supports, love and endurance, I would not be able to move on against all odds in completing this academic research journey.

ABSTRACT

Cloud computing is a technology through which data can be stored and access at remote server without the installation of software and hardware being done at client side. Security concerns are also very high due to increase in use of cloud computing by the general public. The weakness in user's authentication process and lack of effective security policy in cloud storage leads to many challenges in cloud computing.The two most famous techniques for data security are steganography and cryptography. Utilization of a solitary algorithm is not powerful for extra ordinary state security to information in cloud computing.To improve secure of data in cloud storage by hybrid three algorithms (AES, ECC and RSA).All the existing algorithms has some sort of problems and issues, this had made us decide to develop a safe, correct ad efficient algorithm for having secured data in cloud storage. Encryption before uploading the files to cloud server is highly recommended to make them secure. Double checks are applied when the user uploads the data. It is not done only by encrypting it but also providing access to the data only on successful authentication. ECC, AES, and RSA algorithms will be used to encrypt the files to enhance security data on the cloud storage.Numeric values for Secrecy and Performance are obtained. To perform the required tasks separate Java programs are written. Input data size is varied from 100 MB to 1000 MB. Input is given as text files. Particular input is read by the relevant Java program and the encryption time and secrecy are calculated and output on the screen. Average encryption time and secrecy of cipher are calculated

after 14 files for testing. The aim was to produce two graphical outcomes which show the variation of the Average Encryption Time and Secrecy Value over the input data size.The results show that the new algorithm AES-ECC-RSA (AER) was more secure than the remaining algorithms and it proved to be more secure but needed longer time to encrypt data and decrypt data.

ABSTRAK

Pengkomputeranawanadalahteknologi di mana data bolehdisimpandandiakses di pelayanjauhtanpapemasanganperisiandanperkakasan yang dilakukan di sisipelanggan.Kebimbangankeselamatanjugasangattinggikeranapeningkatanpenggunaanko mputerisasiawanoleh orang awam.Kelemahandalam proses pengesahanpenggunadankurangnyakeselamatandasar yang berkesandalampenyimpananawanmenyebabkanbanyakcabarandalam cloud pengkomputeran. Duateknik yang paling terkenaluntuk data keselamatanialahsteganografidankriptografi.Penggunaanalgoritma solver tidakberkuasauntukkeselamatannegarabiasatambahankepadamaklumatdalamawanpengkom puteran.Untukmeningkatkankeselamatan data dalampenyimpananawandengantigaalgoritma hybrid (AES, ECC dan RSA).Semuaalgoritma yang adamempunyaibeberapamasalahdanmasalah, initelahmembuat kami memutuskanuntukmembangunkancekalgoritma yang cekapdanberkesaniklankeranatelahmengamankan data dalam cloud storage.Penyulitansebelummemuatnaik fail kepelayan cloud sangatdisyorkanuntukmenjadikannyaselamat.

Pemeriksaanbergandadigunakanapabilapenggunamemuatnaik data.Iatidakdilakukanhanyadenganmenyulitkannyatetapijugamenyediakanakseskepada data hanyapadapengesahan yang berjaya. Algoritma ECC, AES, dan RSA akandigunakanuntukmenyulitkan fail untukmeningkatkankeselamatan data padapenyimpananawan.

NilaiangkauntukKerahsiaandanPencapaiandiperolehi.Untukmelaksanakantugas-tugas yang diperlukan, program Java yang berasinganakanditulis. Input data saizberbezadari 100 MB

hingga 1000 MB. Input diberikansebagai fail teks. Khusus input dibacaoleh program Java yang berkaitandanmasapenyulitandankerahasiaandikiradan output padalayar. Waktupenyulitanpuratadanrahsia cipher dikiraselepas 14 gagaluntukujian. Matlamatnyaadalahuntukmenghasilkanduahasilgrafikyang menunjukkanvariasiMasaPenyulitanPuratadanKerahsiaanNilaiberbandingsaiz input data. Keputusanmenunjukkanbahawaalgoritmabaru AES-ECC-RSA (AER) lebihselamatdaripadaalgoritma yang tinggaldaniaterbuktilebihselamattetapimemerlukanlebih lama untukmenyulitkan data danmenyahsulit data.

TABLE of CONTENTS

Approval	I
Declaration	II
Dedication	III
Acknowledgement	I
Abstract	V
Abstrak	V
List of Tables	V
List of Figures	I
CHAPTER 1: INTRODUCTION	X
1.1 Background	X
1.2 Problem Statement	I
1.3 Research Objectives	1
1.4 Scope of the Research	1
1.5 Methodology:	2
1.6 Contributions	2
CHAPTER 2: LITERATURE REVIEW	3
2.1Introduction	3
2.1.1Security	4
2.1.2Cryptosystem	5
2.1.3Symmetric Key Cryptosystem	5
2.1.4 Public Key Cryptosystem	5
2.2 Over previous work	5
2.3 Encryption algorithms	6
2.3.1.1 Advanced Encryption Standard	6
2.3.1.2. Add Round Keys Transformation	6

2.3.1.3. Sub Bytes Transformation 16
2.3.1.4. Shift Rows Transformation 16
2.3.1.5. Mix Columns Transformation 18
2.3.2 Elliptic Curve Cryptography 18
2.3.2.1 Elliptic Curves 20
2.3.2.3 Point Arithmetic 20
2.3.2.4 Definitions 22
2.3.2.5 Addition Properties 21
2.3.2.5 Addition Steps 24
2.3.2.6 Point Negation 24
2.3.2.7 Point Addition 22
2.3.2.8 Point Doubling 25
2.3.3 RSA Algorithm 25
2.3.3.1 Problems In RSA Algorithm 26
2.3.3.2 Advantages Of RSA Algorithm 28
2.4 The Security for algorithm 34
2.4.1 The Security of AES 35
2.4.1.1 Brute Force Attack 35
2.4.1.2 Mathematical Attack 36
2.4.1.3 Timing Attack 36
2.4.2 The Security of RSA 36
2.4.2.1 Brute Force Attack 30
2.4.2.2 Mathematical Attacks 36
2.4.2.3 Timing Attack 37
CHAPTER 3: RESEARCH METHODOLOGY 37
3.1 Introduction 38
3.2 Hybrid Cryptographic Algorithms 38
3.2.1 Hybrid Cryptographic for RSA and ECC Algorithms 40
3.2.1.1 Construction 40
3.2.1.2 Hybrid RSA-ECC Encryption Algorithm 40
3.2.1.3 Hybrid RSA-ECC decryption Algorithm 40
3.2.2 Hybrid RSA-AES Encryption and decryption Algorithms 41
3.2.3 Hybrid AES, ECC and RSA Algorithms (AER) 41
3.2.3.1 Encryption Algorithm for Hybrid AES-ECC-RSA (AER) 42

3.2.3.2. Decryption Algorithm for Hybrid AES-ECC–RSA (AER) 42
3.3. Secrecy of Ciphers 45
3.3.1. Definition of 'entropy' 45
3.3.2. Definition of 'uncertainty' 46
3.3.3. Definition of secrecy 48
3.4 Methodology and Implementation 48
3.4.1. Implementation for Execution Time 48
3.4.2 Implementation of testing the security 49
3.4.2.1 Method of testing 49
3.4.2.2 How the secrecy is calculated 49
3.5 The comparative and the results for executing time and security 51
3.5.1 The implementation for encryption algorithms 52
3.5.2 The implementation for decryption algorithms 53
3.6 The experimental results and comparison 54
3.6.1 Executing time comparison 54
3.6.2 Security comparison 55
56
CHAPTER 4: CONCLUSION AND FUTURE WORK 59
REFERENCES 62

LIST of TABLES

Table No.	Page
Table 1.Show the file size and results for encryption algorithms	54
Table2. Show the file size and results for decryption algorithms	55
Table3. Show the file size and results for Security value	59

LIST of FIGURES

Figure No.	Page
Figure 1: Methodology diagram	4
Figure 2: : AES Encryption Block Diagram	17
Figure 3: AES Decryption Block Diagram	17
Figure 4: State Matrix Operation	18
Figure 5 : AES Encryption and Decryption	22
Figure 6: Point Addition on an Elliptic Curve	32
Figure 7: Flow of Encryption Algorithm Used in Implementation	44
Figure 8: Encryption and Decryption Diagram for AES-ECC-RSA Algorithm	47
Figure 9: The performance analysis for encryption AES, ECC and RSA	55
Figure 10: the performance analysis for decryption AES, ECC and RSA	51
Figure 11: Comparison encryption time	58
Figure 12: Comparison decryption time	59
Figure 13: Comparison security rate	60

CHAPTER 1

INTRODUCTION

1.1 . Background:

According to [1] ,Cloud computing is a "new" computer model that allows using remote services through a network using various resources. It is basically meant to give maximum with the minimum resources. Cloud computing is one of the latest technologies in IT sector and through cloud storage, one can access data anytime from anywhere.

Security in cloud computing includes ideas, for example, organize security, hardware and control methodologies sent to ensure information, applications and foundation related with cloud computing [2]. An imperative part of cloud is the idea of interconnection with different materials which makes it difficult and fundamental to secure these situations.

In 2001, National Institute of Standards and innovation has set up the detail for the encryption of electronic information; it is known as the Advanced Encryption Standard (AES), [3].

One of the approaches to public key cryptography is Elliptic curve cryptography. They are based on the algebraic structure of elliptic curves over finite fields based on [2]

Rivest Shamir Adleman (RSA)a public key encryption algorithm developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 that became a de facto standard. Pretty Good privacy that is known as PGP is one of the encryption program that has been formed on the basis of RSA. RSA is an algorithm for public key encryption. RSA algorithm has changed the history by providing both features that is encryption and signing. It involves three steps: key generation, encryption and decryption It is still widely used in electronic commerce protocols, and is believed security depends on the difficulty of decomposition of large numbers [4].

1.2. Problem Statement:

Cloud computing is a technology through which data can be stored and access at remote server without the installation of software and hardware being done at client side. Security concerns are also very high due to increase in use of cloud computing by the general public. The weakness in user's authentication process and lack of effective security policy in cloud storage leads to many challenges in cloud computing [2].The two most famous techniques for data security are steganography and cryptography. Utilization of a solitary algorithm is not powerful for extra ordinary state security to information in cloud computing [5].

1.3. Research Objective:

To improve secure of data in cloud storage by hybrid three algorithms (AES, ECC and RSA).

1.4. Scope of the study:

Evaluation of three hybrid cryptography techniques is to be done in this study. The three algorithmsinclude ECC, RSA, and AES algorithm. This is to be done in order to improve Security of Data in Cloud Storage.

1.5. Methodology:

All the existing algorithms has some sort of problems and issues, this had made us decide to develop a safe, correct ad efficient algorithm for having secured data in cloud storage. Encryption before uploading the files to cloud server is highly recommended to make them secure.Double checks are applied when the user uploads the data. It is not done only by encrypting it but also providing access to the data only on successful authentication. ECC,AES, and RSA algorithms will be used to encrypt the files to enhance security data on the cloud storage.

The three stages of this algorithm include:

- The first phase encrypts Clair text with AES Algorithm.
- In the second stage, encryption of cipher text1 with ECC Algorithm is done.
- The third phase encrypts cipher text1 with RSA Algorithm.

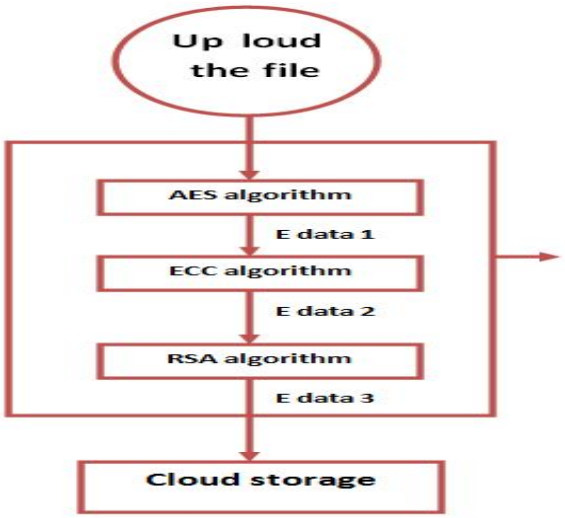

Fig .1: Methodology diagram

1.6. Contributions:

In this research some facts will be found out that contribute to the body of knowledge and these expected facts can be summarized as such:

1. The data stored in the cloud storage more security.
2. Strong encrypted data.

REFERENCES

[1] A. Azougaghe, Z. Kartit, M. Hedaboui, M. Belkasmi, and M. E. L. Marraki, "An efficient algorithm for data security in cloud storage."

[2] S. Singh and V. Kumar, "Secured User's Authentication and Private Data Storage-Access Scheme in Cloud Computing Using Elliptic Curve Cryptography," *Comput. Sustain. Glob. Dev. (INDIACom), 2015 2nd Int. Conf.*, pp. 791–795, 2015.

[3] Federal Information Processing Standards Publications (FIPS), "Advanced Encryption Standard," no. FIPS PUB 197, 2001.

[4] G. Singh, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," *Int. J. Comput. Appl.*, vol. 67, no. 19, pp. 975–8887, 2013.

[5] G. Prabuttt, "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud," pp. 3688–3693, 2016.

[6] D. Coppersmith, "The Data Encryption Standard (DES) and its strengths against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, 1994.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[8] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of Data Encryption Standard," *Int. Test Conf.*, pp. 339–344, 2004.

[9] Z. A. Hussien *et al.*, "Public Auditing for Secure Data Storage in Cloud through a Third Party Auditor Using Modern Ciphertext," pp. 73–78, 2015.

[10] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing A Secure Cloud Storage System for Storing IoT Data by Applying Role Based

Encryption," *Procedia Comput. Sci.*, vol. 89, pp. 43–50, 2016.

[11] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems," *J. Netw. Comput. Appl.*, vol. 59, pp. 208–218, 2016.

[12] W. Song, B. Wang, Q. Wang, Z. Peng, W. Lou, and Y. Cui, "A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications," *J. Parallel Distrib. Comput.*, vol. 99, pp. 14–27, 2017.

[13] X. Yin, Z. Liu, Y. S. Lee, and H. J. Lee, "PKI-based cryptography for secure cloud data storage using ECC," *2014 Int. Conf. Inf. Commun. Technol. Converg.*, pp. 194–199, 2014.

[14] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.

[15] P. Prajapati, N. Patel, R. Macwan, N. Kachhiya, and P. Shah, "Comparative Analysis of DES , AES , RSA Encryption Algorithms," no. 1, pp. 132–134, 2014.

[16] Y. Wang and M. Hu, "Timing evaluation of the known cryptographic algorithms," *CIS 2009 - 2009 Int. Conf. Comput. Intell. Secur.*, vol. 2, pp. 233–237, 2009.

[17] V. R. Pancholi, "Enhancement of Cloud Computing Security with Secure Data Storage using AES," *Int. J. Innov. Res. Sci. Technol.*, vol. 2, no. 9, pp. 18–21, 2016.

[18] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, 2016.

[19] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: Des and AES," *2012 IEEE Students' Conf. Electr. Electron. Comput. Sci. Innov. Humanit. SCEECS 2012*, 2012.

[20] A. Al Hasib and A. A. M. M. Haque, "A comparative study of the performance and security issues of AES and RSA cryptography," *Proc. - 3rd Int. Conf. Converg. Hybrid Inf. Technol. ICCIT 2008*, vol. 2, no. November 2001, pp. 505–510, 2008.

[21] K. Rege, N. Goenka, P. Bhutada, and S. Mane, "Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA," vol. 71, no. 22, pp. 10–13, 2013.

[22] M. B. Vishnu, S. K. Tiong, M. Zaini, and S. P. Koh, "Security enhancement of digital motion image transmission using hybrid AES-DES algorithm," *2008 14th Asia-Pacific Conf. Commun.*, 2008.

[23] W. Tianfu and K. Babuttt, "Design of a Hybrid Cryptographic Algorithm," *Int. J. Comput. Sci. ...*, vol. 2, no. 2, pp. 277–283, 2012.

[24] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–203, 1987.

[25] V. Miller, "Use of Elliptic Curves in Cryptography," *Adv. Cryptol. – CRYPTO'85*, vol. LNCS 218, pp. 417–426, 1986.

[26] G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, "2 : The Rijndael algorithm," *Symp. A Q. J. Mod. Foreign Lit.*

[27] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 12, no. 9, pp. 957–967, 2004.

[28] D. Patel, "Data Security In Cloud Computing Using Digital Signature."

[29] S. R. Lenka and B. Nayak, "Enhancing Data Security in Cloud Computing Using RSA Encryption and MD5 Algorithm," vol. 2, no. 3, pp. 60–64, 2014.

[30] V. B. P.V.NITHYABHARATHI, T.KOWSALYA, "To Enhance Multimedia Security in Cloud Computing Environment Using RSA and AES," *Int. J. Sci. Eng.*

Technol. Res., vol. 3, no. 2, 2014.

[31] R. Kaur and R. P. Singh, "Enhanced cloud computing security and integrity verification via novel encryption techniques," *Proc. 2014 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2014*, pp. 1227–1233, 2014.

[32] S. Belguith, A. Jemai, and R. Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm," in *The Eleventh International Conference on Autonomic and Autonomous Systems, ICAS*, 2015, pp. 98–103.

[33] R. Titare and P. Kulurkar, "Data Security and Privacy in Cloud using RC6 Algorithm for Remote Data Back-up Server," *Ijesat.Org*, no. 2, pp. 149–153.

[34] S. Kaushik and C. Gandhi, "Cloud data security with hybrid symmetric encryption," *2016 Int. Conf. Comput. Tech. Inf. Commun. Technol. ICCTICT 2016 - Proc.*, pp. 636–640, 2016.

[35] S. Kaur, "Multi-Level Data Integrity Service," *Int. J. Comput. Appl.*, vol. 103, no. 14, p. 8887, 2014.

[36] S. B. Subhash, "Data Confidentiality in Cloud Computing with Blowfish Algorithm," *Int. J. Emerg. Trends Sci. Technol.*, vol. 1, no. 1, pp. 1–6, 2014.

[37] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," pp. 185–194.

[38] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[39] F. Fatemi Moghaddam, M. T Alrashdan, and O. Karimi, "A Hybrid Encryption Algorithm Based on RSA Small-e and Efficient-RSA for Cloud Computing Environments," *J. Adv. Comput. Networks*, vol. 1, no. 3, pp. 238–241, 2013.

[40] N. Kaaniche, A. Boudguiga, and M. Laurent, "ID based cryptography for cloud data

storage," *IEEE Int. Conf. Cloud Comput. CLOUD*, pp. 375–382, 2013.

[41] N. R. Potlapally, S. Ravi, A. Raghunathan, and G. Lakshminarayana, "Optimizing public-key encryption for wireless clients," *2002 IEEE Int. Conf. Commun. Conf. Proceedings. ICC 2002 (Cat. No.02CH37333)*, vol. 2, pp. 1050–1056, 2002.

[42] A. Nadeem and M. Y. Javed, "Comparison of," *2005 Int. Conf. Inf. Commun. Technol.*, pp. 84–89, 2005.

[43] D. Elminaam, "Performance evaluation of symmetric encryption algorithms," *Int. J. Comput. Networks*, vol. 8, no. 12, pp. 280–286, 2008.

[44] A. Sachdev and M. Bhansali, "Enhancing cloud computing security using aes algorithm," *Int. J. Comput. Appl.*, vol. 67, no. 9, p. 8887, 2013.

[45] S. P. Jadhav and B. R. Nandwalkar, "Efficient Cloud Computing with Secure Data Storage using AES," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 4, no. 6, pp. 2–6, 2015.

[46] R. S. Ghavghave and D. M. Khatwar, "Architecture for Data Security in Multi-Cloud Using AES-256 Encryption Algorithm," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 3, no. 5, pp. 157–161, 2015.

[47] R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," *Int. J. Eng. Res. Appl.*, vol. 3, no. 4, pp. 1922–1926, 2013.

[48] A. Castiglione, M. Cepparulo, A. De Santis, and F. Palmieri, "Towards a lawfully secure and privacy preserving video surveillance system," *Lect. Notes Buttts. Inf. Process.*, vol. 61 LNBIP, pp. 73–84, 2010.

[49] D. Bleichenbacher, M. Ave, and M. Hill, "Chosen Ciphertext Attacks Against Protocols B a s e d on t h e R S A E n c r y p t i o n Standard PKCS."

[50] J. Daemen, V. Rijmen, and K. U. Leuven, "AES Proposal : Rijndael," *Complexity*,

pp. 1–45, 1999.

[51] O. Systems and P. C. Kocher, “Timing Attacks on Implement at ions of,” *Advances*, pp. 104–113, 1996.