International Journal of Inventive Engineering and Sciences

ISSN : 2319- 9598
Website: www.ijies.org
Volume-4 Issue-10, JUNE 2018
Published by:
Blue Eyes Intelligence Engineering and Sciences Publication Pvt.

Dr. Labib Francis Gergis Rofaiel
Associate Professor, Department of Digital Communications and Electronics, Misr Academy for Engineering and Technology, Mansoura, Egypt.

Dr. Hugo A.F.A. Santos
ICES, Institute for Computational Engineering and Sciences, The University of Texas, Austin, USA.

Dr. Sunandan Bhunia
Associate Professor & Head, Department of Electronics & Communication Engineering, Haldia Institute of Technology, Haldia (Bengal), India.

Dr. Awatif Mohammed Ali Elsiddieg
Assistant Professor, Department of Mathematics, Faculty of Science and Humatarian Studies, Elnielain University, Khartoum Sudan, Saudi Arabia.

Technical Program Committee Chair

Dr. Mohd. Nazri Ismail
Associate Professor, Department of System and Networking, University of Kuala (UniKL), Kuala Lumpur, Malaysia.

Technical Program Committee Members

Dr. Haw Su Cheng
Faculty of Information Technology, Multimedia University (MMU), Jalan Multimedia (Cyberjaya), Malaysia.

Dr. Hasan. A. M Al Dabbas
Chairperson, Vice Dean Faculty of Engineering, Department of Mechanical Engineering, Philadelphia University, Amman, Jordan.

Dr. Gabil Adilov
Professor, Department of Mathematics, Akdeniz University, Konyaaltı/Antalya, Turkey.

Dr. Ch.V. Raghavendran
Professor, Department of Computer Science & Engineering, Ideal College of Arts and Sciences Kakinada (Andhra Pradesh), India.

Dr. Thanhtrung Dang
Associate Professor & Vice-Dean, Department of Vehicle and Energy Engineeering, HCMC University of Technology and Education, Hochiminh, Vietnam.

Dr. Wilson Udo Udofia
Associate Professor, Department of Technical Education, State College of Education, Afaha Nsit, Akwa Ibom, Nigeria.

Convener Chair

Mr. Jitendra Kumar Sen
Blue Eyes Intelligence Engineering & Sciences Publication Pvt. Ltd., Bhopal(M.P.), India

Editorial Chair

Dr. Sameh Ghanem Salem Zaghloul
Department of Radar, Military Technical College, Cairo Governorate, Egypt.

Editorial Members

Dr. Uma Shanker
Professor, Department of Mathematics, Muzafferpur Institute of Technology, Muzafferpur(Bihar), India

Dr. Rama Shanker
Professor & Head, Department of Statistics, Eritrea Institute of Technology, Asmara, Eritrea

Dr. Vinita Kumar
Department of Physics, Dr. D. Ram D A V Public School, Danapur, Patna(Bihar), India

Dr. Brijesh Singh
Senior Yoga Expert and Head, Department of Yoga, Samutakarsha Academy of Yoga, Music & Holistic Living, Prahladnagar, Ahmedabad (Gujarat), India.

Dr. J. Gladson Maria Britto
Professor, Department of Computer Science & Engineering, Malla Reddy College of Engineering, Secunderabad (Telangana), India.

Dr. Sunil Tekale
Professor, Dean Academics, Department of Computer Science & Engineering, Malla Reddy College of Engineering, Secunderabad (Telangana), India.

1.

Authors: Aishwarya Rathod, Bhagyalaxmi Kodre, Nida Sayyed, Ronak Sayta, Lata Sankpal

Paper Title: Implementation of Location Based Encryption for Secure Banking Transactions in Mobile Data Environment

Abstract: Security has constantly been a fundamental bit of human life. People have been hunting down physical and monetary security. With the progression of human learning and getting into the new period the need of data security were added to human security concerns. Information is encoded just when individual is having private key. In cryptography "character" part is imperative, we can utilize this part as encryption. Those are inside specific topographical zone is endorsed for information decoding, otherwise not permitted. Another utilization of "Location Based Cryptography" is get to control. (Ex-getting to printer in a room however can't access outside of room.). It is more suitable for banks, enormous organizations, Institutions.

Keywords: Authentication, Banking Application, GPS, LDEA, Shoulder Surfing, Security

References:

1. Aishwarya Rathod, Bhagyalaxmi Kodre, Nida Sayyed, Ronak Sayta and Prof. Lata Sankpal, "Location Based Encryption for Secure Banking Transactions in mobile data environment" IJAERD, e-ISSN (O): 2348-4470, p-ISSN (P): 2348-6406, Volume 4, Issue 11, November -2017.
2. Aishwarya Nair, Ankita Devrukhar, Karthika M. Vinod, Pallavi Lanke, "Protected Mobile Banking Using Location of Users", IJARCCE, ISO 3297:2007 Certified, Vol. 6, Issue 4, April 2017.
3. Sourish Mitra, Avijit Chakrabotry, Arunabha Bhaumik, Joy Devanjee, Mainak Maulik, "A location dependent cryptographic approach based on target coordinate from distanc tolarant key transfer for GPS mobile reciever", IOSR-JCe, e-ISSN: 2278-0661, p-ISSn:2278-8727, Volume 17, Issue 1, Ver.VI 2015, pp 56-63.
4. Mohammad Ahmdian, Jalal Khodabandeloo, Dan C. Marinescu, "A security scheme for geographic information databases in location based system",IEEE southeast conference, 2015, Florida.
5. Y. Lakshmi Prasanna, Prof. E. Madhusudhan Reddy, "A Generalized Study on Encryption Techniques for Location Based Services",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 19-26,2014.
6. Amit Kushwaha, Vineet Kushwaha, "Location based services using android mobile operating System", Int. J. Adv. Eng. Technol., vol. 1,no. 1, pp. 1420, 2011.
7. Hamad Hatem, Elkourd Souhir, "Data encryption using the dynamic location and speed of mobile node", European, Mediterranean & MiddleEastern Conference on Information Systems 2010 (EMCIS2010) April 12-13 2010, Abu Dhabi, UAE.
8. Sandeep Kumar, Mohammed Abdul Qadeer, Archana Gupta, "Location based services using Android", Proc. IEEE Int. Conf. Soc. Comput., 2012, pp. 471480,2009.
9. Hsien-Chou Liao and Yun-Hsiang Chao, "LDEA: Data encryption algorithm based on location of mobile users",Taiwan(R.O.C.), Journal 2008, Vol. 7, No. 1, p. 63-69.
10. Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang, "Securing sensor networks with location-based keys", IEEE communication society/WCNC 2005, 0-7803-8966-2/05/$20.00 2005 IEEE.
11. Christian Becker, Frank Durr, "On location models for ubiquitous computing", 2005 9: 20-31, DOI: 10.1007/s00779-004-0270-2,2003.
12. William Enck, Peter Gilbert, Byung-Gon Chun, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones", Proc. 9th USENIX Conf. Oper. Syst.Des. Implementation, 2010, pp. 1–6.
13. Tomas Sander Christian, F. Tschudin, "Towards Mobile Cryptography", International Computer Science Institute, Berkeley, icsi.berkeley.edu

2.

Authors: Priyanka Pandey, R. R. Sedamkar

Paper Title: Hybrid AES Algorithm with Enhanced Security for Heterogeneous Data

Abstract: This paper, presents the intricate Hybrid AES encryption method. Proposed algorithm's design and evaluation of security enhancement is done by implementing and comparing Dynamic S-box with Round structure & Variable Key Cipher technique for heterogeneous data. AES is one of ciphering algorithm which is utilized for encryption, decryption of data to provide confidentiality for end to culminate data transmission. Improvement is finished in AES by modifying the S-box. The static S-box is created dynamic utilizing key programing with the repetition of variable cipher key. The improvement analysis relies on cryptography Time, decoding Time and Throughput. Performance enhancement for security is evaluated for all the four algorithms- AES, AES with Round structure, AES with Variable Key cipher and our proposed Hybrid algorithm- AES with Round Structure and Variable key Cipher. Here focus is to make system attack resistant & secure data from assailers.

Keywords: AES; S-box; Dynamic S-box, Round structure, Variable Key Cipher.

References:

1. T. T. K. Hue T. M. Hoang and D. Tran, "Chaos-based S-box for lightweight block cipher//Communications and Electronics (ICCE)", IEEE Fifth International Conference IEEE, 2014.
2. Guo Guang-liang, Qian Quan, Zhang Rui, "Different Implementations of AES Cryptographic Algorithm," High Performance Computing and Communications (HPCC), (CSS), and (ICESS) 2015 IEEE 17th International Conference, 2015.
3. Scripcariu, L., "A study of methods used to improve encryption algorithms robustness," in Signals, Circuits and Systems (ISSCS) IEEE, 2015.
4. Nilesh D., Nagle M., "The new cryptography algorithm with high throughput," in Computer Communication and Informatics (ICCCI) IEEE, 2014
5. Chhotaray, S.K.; Chhotaray, A.; Rath, G.S., "A new method of generating public key matrix and using it for image encryption," in Signal Processing and Integrated Networks (SPIN), IEEE, 2015.
6. Schneider, Computer-and-network-security. WilsoN Publications, 2014. [28] Ed Skoudis, Top-computer and- network-security. Mc Graw Hill, 2015.
7. L. Stein, "Random patterns," in Computers and You, J. S. Brake, Ed. New York: Wiley, 1994, pp. 55-70.

8. Transmission Systems for Communications, 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.
9. Karsanbhai, G.R, Shajan, M.G, "128 bit AES implementation for secured wireless communication," in Emerging Trends in Networks and Computer Communications (ETNCC),IEEE , 2011
10. S. Sahmod, W. Elmastry, S. Abudalta, "Enhance the Security of AES Against Modern Attacks by Using Variable Key Block Cipher" in International Arab Journal of e-technology, 2013
11. Daemen, "The Design of Rijndael-Advanced Encryption Standard", Nature 618.7532 (2015): 109110.
12. http://www.onlineprogrammingbooks.com/itsecurityaccessed 25-12-2016, 12:54 pm.
13. http://www.garykessler.net/library/crypto.htmlaccessed 25-12-2016, 12:58 am.

3.

Authors: **R. Prakash Rao**

Paper Title: **Various Power Dissipation Techniques for CMOS Inverter**

Abstract: Low power design of complex CMOS circuits is one of the major challenges that is being addressed and will be addressed in nanometer design era. With integration of millions and billions of transistors on a single chip, transistor density is drastically increasing that lead to more and more complexity in applications being implemented on a single chip. Design time is another major challenge that forces designers to address the need in a very short time optimizing chip performances. In order to ensure that the design is through in the first iteration, designers are banking on new methodologies and readymade solutions to optimize area, time and power. Hence, various power dissipation techniques for CMOS inverter circuit are investigated here.

Keywords: Low Power Design, CMOS Circuits, Millions and Billions of Transistors, Transistor Density, Optimize Area, Time and Power.

References:

1. Thomas Olsson, Peter Nilsson, Thomas Meincke (2000), "ADigitally Controlled Low-Power Clock Multiplier for Globally Asynchronous Locally Synchronous Designs", ISCAS2000, IEEE Int. Symp., Circuits and Systems, Geneva,
2. Fayed. A.A, Bayoumi. M.A (2001), "A novel architecture for low-power design of parallel multipliers", VLSI Proc., IEEE Computer Society Workshop, pp. 149 – 154, May 2001.
3. In-Chung Hwang, Sang-Hun Song, Soo-Won Kim (2001),"A Digitally Controlled Phase- Locked Loop with a Digital Phase-Frequency Detector for Fast Acquisition", IEEE JSSC, vol. 36, pp. 1574-1581, Oct.2001.
4. Ming-Chung Tang, R.C. Chang, Wei-Kuan Shih (2001), "Software Radio System Design for Accessing Wireless Multimedia Services", Int., Journal of Computer Research on Advances in Information Processing and Technology, vol. 10, no. 3, pp. 347 - 360, 2001.
5. John. Proakis (2001), "Digital Communications", Fourth Edition, Mc.GH. pub
6. Schwarzbacher A.Th., Silvennoinen J.P, Comiskey P.A (2002), "Benchmarking CMOS Adder Structures", Irish Systems and Signal Conference, Cork, Ireland, pp. 231 – 234, June 2002.

12-14