UNIVERSITAS
GADJAH MADA
**Implementasi Algoritme RSA pada Field Programmable Gate Array (FPGA) menggunakan Algoritme Montgomery**
ESTI KURNIASARI, Agfianto Eko Putra, Dr., M.Si.;Nia Gella Augoestien, S.Si.,M.Cs.
**Universitas Gadjah Mada, 2018 | Diunduh dari http://etd.repository.ugm.ac.id/**

# DAFTAR PUSTAKA

Acar. T., dan Kaliski. B. S., 1996, Analyzing and Comparing Montgomery Multiplication Algorithms, in IEEE Micro, vol. 16, no. 3, pp. 26-33, June 1996, shttps://ieeexplore.ieee.org/abstract/document/502403/

Ambika, R., Samachandran, S., dan Kashwan, K.R., 2014, Design of Commutative Cryptography Core with Key Generation for Distributed FPGA Architecture, *International Journal of Current Engineering Technology,* 2277-4106, 4, 3519-3527, http://inpressco.com/wp-content/uploads/2014/10/Paper783519-3527.pdf.

_____, 2013, Securing Distributed FPGA System using Commutative RSA Core; *Global Journal of Researches in Engineering Electrical and electronics Engineering*, vol. 13, issue 15, pp.47-58, https://globaljournals.org/item/2648-securing-distributed-fpga-system-using-commutative-rsa-core

Anand, A. dan Praveen, P., 2012, Impementation of RSA Algorithm on FPGA, *International Journal of Engineering Research & Technology (IJERT)*, vol1, issue5, 1-7, https://www.ijert.org/phocadownload/V1I5/IJERTV1IS5454.pdf.

Ashenden, P.J., 2008, *The Designer's Guide to VHDL*, 3th edition, volume 3, Elsevier Inc, Burlington.

Brown, S dan Vranesic, Z., 2009, *Fundamental Digital Logic with VHDL Design*, edisi ketiga, The McGraw-Hill Companies, Toronto.

Chu, P.P., 2008, *FPGA Prototyping by VHDL Examples: Xilinx Spartan$^{TM}$-3 Version*, John Wiley & Sons, Inc., Canada.

Deschamps, J., Bioul, G.J.A., dan Sutter, G.D., 2006, *Synthesis of Arithmetic Circuits,* Wiley-Interscience.

Dongjiang, T., Yandan, W., dan Hong, C., 2012, The research on key generation in RSA public-key cryptosystem, *Fourth International, Conference on Computational and Information Sciences*,17-19 Agustus, 578-580, Beijing.

Gaspar. L., 2014, FPGA performances in Cryptography, *Performance analysis of different cryptographic algorithms implemented in an FPGA*, Joint Research Centre, Institute for the Protection and Security of the Citizen, Luxembourg.

Hanindhito, B., Ahmadi, N., Hogantara, H., Arrahmah, A.I., dan Adiono, T., 2015, FPGA Implementation of Modified Serial Montgomery Modular Multiplication for 2048-bit RSA, *International Seminar on Intelligent Technology and Its Appliction*, 20-21 Mei, 113-118, Surabaya, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7219964&isnumber=7219932.

UNIVERSITAS
GADJAH MADA
**Implementasi Algoritme RSA pada Field Programmable Gate Array (FPGA) menggunakan Algoritme Montgomery**
ESTI KURNIASARI, Agfianto Eko Putra, Dr., M.Si.;Nia Gella Augoestien, S.Si.,M.Cs.
**Universitas Gadjah Mada, 2018 | Diunduh dari http://etd.repository.ugm.ac.id/**


Heri, K. I., Bagja N. A., Randi S., Purba, dan Adion, T., Very Fast Pipelined RSA Architecture Based on Mntgomery's Algorithm, *International Conference on Electrical Engineering and Informatics*, 5-7 Agustus, Selangor.

Iana, G. V., Anghelescu, P., dan Serban, G., 2011, RSA encryption algorithm implemented on FPGA, Applied Electronics (AE), *2011 International Conference*, 7-8 September, 1-4, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6049062&isnumber=6048828.

Kromodimoeljo, S., 2010, *Teori dan Aplikasi Kriptografi*, SPK IT Consulting.

Landge, A.R. dan Ansari, A.H., 2013, RSA Algorithm realization on FPGA, *International Journal of Advance Reasearch in Computer Enginering & Technology (IJARCET),* 2275-1323, 2, 2323-2327, http://ijarcet.org/wp-content/uploads/IJARCET-VOL-2-ISSUE-7-2323-2327.pdf.

Leelavathi, G., Shaila, K., dan Venugapol, K.R., 2016, Elliptic Curve Cryptography Implementation on FPGA using Montgomery Multiplication for Equal Key and Data Size over GF($2^m$) for Wireless Sensor Networks, *Proceedings of the International Conference,* Bengaluru, India.

Liu, Z., Xia, L., Jing, J., dan Liu. P., 2011, A Tiny RSA Coprcessor Based in Optimized Systolic Montgomery Architecture, *Security and Cryptography (SECRYPT)*, 18-21 Juli.

Henriquez, F. R., Saqib, N. A., Diaz-Perez, A., dan Koc, C. K., 2006, Cryptographic Algorithms on Reconfigurable Hardware, United States of America, Springer.

Sharma, S. dan Zodpe, H., 2016, *Implementation of Cryptography Algorithm for E-Passport Security*, 26-17 Agustus, Pune, India, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7830150&isnumber=7830057.

Singh, S. dan Jassal, P. S., 2016., Synthesis and Analysis of 32-bit RSA Algorithm Using VHDL, *International Journal of Enginering Science,* 2320-0332, 17, 310-315, http://ijoes.vidyapublications.com/paper/Vol17/45-Vol17.pdf.

Skobic, V., Dokic, B., Ivanovic, Z., 2014, Hardware Modules of the RSA Algorithm, *Serbian Journal of Electrical Engineering*, No. 1, Vol. 11, 121-131, http://www.doiserbia.nb.rs/img/doi/1451-4869/2014/1451-48691400011S.pdf.

Stallings. W., 2014, *Cryptography and Network Security: Principles and Practice*, Edisi 6, Prentice Hall, New York.

Sun, H. dan Ding, Q., 2015, The design of mobile phone module information encryption system based on FPGA, *Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control,* Harbin, China.

UNIVERSITAS
GADJAH MADA
**Implementasi Algoritme RSA pada Field Programmable Gate Array (FPGA) menggunakan Algoritme Montgomery**
ESTI KURNIASARI, Agfianto Eko Putra, Dr., M.Si.;Nia Gella Augoestien, S.Si.,M.Cs.
**Universitas Gadjah Mada, 2018 | Diunduh dari http://etd.repository.ugm.ac.id/**


Syahral, M., 2011, Perancangan dan Implementasi Algoritme Enkripsi Arcfour pada Perangkat Kriptografi Berbasis FPGA, *Skripsi*, Fakultas Teknik Elektro, Universitas Indonesia, Depok.

Tahir, A.S., 2015, Design and Implementation of RSA Algorithm using FPGA, *International Journal of Computer & Technology*, 12, 14, 6361-6367, https://www.researchgate.net/publication/282249995_Design_and_Implementation_of_RSA_Algorithm_using_FPGA

Thobbi, A., Dhage, S., Jadhav, P., dan Chandrachood, A., 2015, Implementation of RSA Encryption Algorithm on FPGA, *American Journal od Enginering Reasearch (AJER),* 6, 4, 144-151, http://www.ajer.org/papers/v4(06)/Q04601440151.pdf.

https://www.xilinx.com/support/documentation/university/XUP%20Boards/XUPNexys4/documenatation/Nexys4_RM_VB1_Final_3.pdf

https://www.xilinx.com/support/answers/57304.html