DAFTAR PUSTAKA

Afianah, N., Eko Putra, A., Dharmawan, A., 2019. High-Level Synthesize of Backpropagation Artificial Neural Network Algorithm on the FPGA. Int. Conf. Sci. Technol. ICST.

Alejandro, C., 2012. FPGA Introduction. Lecture Notes : http://indico.ictp.it/event/a11204/session/7/contribution/4/material/0/0.pdf

Augoestien, N.G., Putra, A.E., 2015. Purwarupa Perangkat Keras untuk Eksekusi Algoritma AES Berbasis FPGA. IJEIS Indones. J. Electron. Instrum. Syst. 5, 211. https://doi.org/10.22146/ijeis.7644

Barkalov, A., Titarenko, L., Mielcarek, K., Chmielewski, S., 2019. Logic Synthesis for FPGA-Based Control Units. Springer.

Blocks, L., 2000. Field Programmable Gate Arrays. http://www.eng.auburn.edu/~strouce/class/elec4200/FPGAoverview.pdf

Chu, P.P., 2006. RTL Hardware Design Using VHDL : Coding for Efficiency, Portability, and Scalability. John Wiley Sons Inc.

Deschamps, J.-P., 2009. Hardward implementation of finite-field arithmetic. McGraw-Hill Professional, Maidenhead.

Deschamps, J.-P., Sutter, G.D., Cantó, E., 2012. Guide to FPGA Implementation of Arithmetic Functions, Lecture Notes in Electrical Engineering. Springer Netherlands, Dordrecht. https://doi.org/10.1007/978-94-007-2987-2

Duan, C., Liu, Y., Chen, Y., 2009. A 3-Stage Pipelined Large Integer Modular Arithmetic Unit for ECC, in: 2009 *International Symposium on Information Engineering and Electronic Commerce*. Presented at the 2009 *International Symposium on Information Engineering and Electronic Commerce*, IEEE, Ternopil, Ukraine, pp. 519–523. https://doi.org/10.1109/IEEC.2009.115

Farooq, U., Marrakchi, Z., Mehrez, H., 2012. FPGA Architectures: An Overview, in: Tree-Based Heterogeneous FPGA Architectures. Springer New York, New York, NY, pp. 7–48. https://doi.org/10.1007/978-1-4614-3594-5_2

Harris, D.M., Harris, S.L., 2013. Digital Design and Computer Architecture. Elsevier.

Kurniasari, E., Putra, A.E., Augoestien, N.G., 2019. Implementation of the Montgomery Modular based RSA Algorithm on FPGA. 2019 5th Int. Conf. Sci. Technol. ICST. https://doi.org/10.1109/ICST47872.2019.9166353

Leininger, J.C., Phillips, G., 1978. 73) Assignee: International Business Machines 19.

Li, J., Dai, Z., Li, W., Yi, S., Zhou, S., 2017. Research and design of add-based length-scalable dual-field modular multiplication-addition-subtraction, in: 2017 2nd IEEE I*nternational Conference on Integrated Circuits and Microsystems* (ICICM). Presented at the 2017 2nd IEEE *International Conference on Integrated Circuits and Microsystems* (ICICM), IEEE, Nanjing, pp. 48–52. https://doi.org/10.1109/ICAM.2017.8242136

Mehlhorn, K., Sun, H., 2013. Lecture 10: Public Key Cryptography 4.

Ruohonen, K., 2014. Mathematical Cryptology.

Savaš, E., Tenca, A.F., Koç, Ç.K., 2000. A Scalable and Unified Multiplier Architecture for Finite Fields GF(p) and GF(2m), in: Koç, Ç.K., Paar, C. (Eds.), Cryptographic Hardware and Embedded Systems — CHES 2000. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 277–292. https://doi.org/10.1007/3-540-44499-8_22

Savugathali, S., Mustapa, M., Sharazel Razali, M., Faiz Zakaria, F., 2019. Timing violation reduction in the fpga prototyped design using failed path fixes and time borrowing techniques. Indones. J. Electr. Eng. Comput. Sci. 14, 628–636. https://doi.org/10.11591/ijeecs.v14.i2.pp628-636

Schueffel, P., Groeneweg, N., Baldegger, R., 2019. The Crypto Encyclopedia. Growth, Switzerland.

Serrano, J., 2008. Introduction to FPGA design 17. https://doi.org/10.5170/CERN-2008-003.231

Stojcev, M.K., Milovanovic, E.I., Milovanovic, I.Z., 2012. A unified approach in manipulation with modular arithmetic, in: 2012 28th *International Conference on Microelectronics Proceedings*. Presented at the 2012 28th *International Conference on Microelectronics* (MIEL 2012), IEEE, Nis, Serbia, pp. 423–426. https://doi.org/10.1109/MIEL.2012.6222892

Trimberger, S.M., 1994. Field-Programmable Gate Array Technology. Springer US, Boston, MA.

Vollala, S., Begum, B.S., Joshi, A.D., Ramasubramanian, N., 2016. High-radix Modular Exponentiation for hardware implementation of Public-Key Cryptography, in: 2016 *International Conference on Computing, Analytics and Security Trends* (CAST). Presented at the 2016 *International Conference on Computing, Analytics and Security Trends* (CAST), IEEE, Pune, India, pp. 346–350. https://doi.org/10.1109/CAST.2016.7914992

Xilinx, 2018. 7 Series DSP48E1 Slice. https://www.xilinx.com/support/documentation/user_guides/ug479_7Series_DSP48E1.pdf

Xilinx, 2016. 7 Series FPGAs Configurable Logic Block. https://www.xilinx.com/support/documentation/user_guides/ug474_7Series_CLB.pdf