Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, London, UK, 2003, pp. 349–365, Springer-Verlag.
[7] Jerome A. Solinas, "Efficient Arithmetic on Koblitz Curves," Des. Codes Cryptography, vol. 19, no. 2-3, pp. 195–249, 2000.
[8] W. N. Chelton and M. Benaissa, "Fast Elliptic Curve Cryptography on FPGA," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 16, no. 2, pp. 198–205, Feb. 2008.
[9] G.Orlando, C.Paar, A high performance reconfigurable elliptic curve processor for GF(2m), Second International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2000), pp 41-56.
[10] Sakyama K, Batina L, Preneel B, et al, Multicore curve-based cryptoprocessor with reconfigurable modular arithmetic logic units over GF(2^n), IEEE Transactions on Computers, vol 56 (9), pp 1269-1282, 2007.
[11] Sozzana F, Bertoni G, S Turcato, et al, A parallelized design for an elliptic curve cryptosystem coprocessor, Proceeding of the International Conference on Information Technology, IEEE Computer Society, pp 626-630, 2005.
[12] Toshiya Itoh and Shigeo Tsujii, "A Fast Algorithm For Computing Multiplicative Inverses in GF(2m) Using Normal Bases," Inf. Comput., vol. 78, no. 3, pp. 171– 177, 1988.
[13] Burton S. Kaliski, "The Montgomery Inverse and its Applications," IEEE Transactions on Computers, vol. 44, no. 8, pp. 1064–1065, 1995.
[14] Francisco Rodríguez-Henríquez, N. A. Saqib, A. Díaz-Pèrez, and Çetin Kaya K¸ oc, Cryptographic Algorithms on Reconfigurable Hardware (Signals and Communication Technology), Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
[15] Parrilla, L.; Lloris, A.; Castillo, E.; García, A., "Minimum-clock-cycle Itoh-Tsujii algorithm hardware implementation for cryptography applications over GF(2m) fields," Electronics Letters , vol.48, no.18, pp.1126,1128, August 30 2012, doi: 10.1049/el.2012.1427
[16] Mahdizadeh, H.; Masoumi, M., "Novel Architecture for Efficient FPGA Implementation of Elliptic Curve Cryptographic Processor Over {\rm GF}(2^{163}) ," Very Large Scale Integration (VLSI) Systems, IEEE Transactions on , vol.21, no.12, pp.2330,2333, Dec. 2013, doi: 10.1109/TVLSI.2012.2230410
[17] Jiafeng Xie; Meher, P.K.; Zhi-hong Mao, "High-Throughput Finite Field Multipliers Using Redundant Basis for FPGA and ASIC Implementations," Circuits and Systems I: Regular Papers, IEEE Transactions on , vol.62, no.1, pp.110,119, Jan. 2015
[18] Azarderakhsh, R.; Jarvinen, K.U.; Mozaffari-Kermani, M., "Efficient Algorithm and Architecture for Elliptic Curve Cryptography for Extremely Constrained Secure Applications," Circuits and Systems I: Regular Papers, IEEE Transactions on , vol.61, no.4, April 2014
[19] JohannesWolkerstorfer, Hardware Aspects of Elliptic Curve Cryptography, Ph.D. thesis, Institute for Applied Information Processing and Communications, Graz University of Technology, 2004.
[20] Anatoly A. Karatsuba and Y. Ofman, "Multiplication of Multidigit Numbers on Automata," Soviet Physics Doklady, vol. 7, pp. 595–596, 1963.
[21] Francisco Rodríguez-Henríquez, N. A. Saqib, A. Díaz-Pèrez, and Çetin Kaya K¸ oc, Cryptographic Algorithms on Reconfigurable Hardware (Signals and Communication Technology), Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
[22] Steffen Peter and Peter Langendörfer, "An efficient polynomial multiplier in GF(2m) and its application to ECC designs," in DATE '07: Proceedings of the conference on Design, automation and test in Europe, San Jose, CA, USA, 2007, pp. 1253–1258, EDA Consortium.
[23] Peter L. Montgomery, "Five, Six, and Seven-Term Karatsuba-Like Formulae," IEEE Transactions on Computers, vol. 54, no. 3, pp. 362–369, 2005.
[24] André Weimerskirch and Christof Paar, "Generalizations of the Karatsuba Algorithm for Efficient Implementations," Cryptology ePrint Archive, Report 2006/224, 2006.
[25] Donald E. Knuth, The Art of Computer Programming Volumes 1-3 Boxed Set, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1998.
[26] Francisco Rodríguez-Henríquez, Guillermo Morales-Luna, Nazar A. Saqib, and Nareli Cruz-Cortés, "Parallel Itoh-Tsujii Multiplicative Inversion Algorithm for a Special Class of Trinomials," Des. Codes Cryptography, vol. 45, no. 1, pp. 19–37, 2007.
[27] Rebeiro, C., Roy, S.S., Reddy, D.S., and Mukhopadhyayy, D.: 'Revisiting the Itho-Tsujii inversion algorithm for FPGA platforms', IEEE Trans. Verg Large Scale Integr. (VLSI) Syst., 2011, 19, (8), pp. 1508–1512
[28] Roy, S.S., Rebeiro, C., and Mukhopadhyay, D.: 'Theoretical modeling of the Itoh-Tsujii inversion algorithm for enhanced performance on k-LUT based FPGAs'. Proc. Design, Automation & Test in Europe Conf. & Exhibition (DATE), Grenoble, France, March 2011, Vol. 1, pp. 1–6

Author Profile

Hemanth R received his B.E in Electronics and communication from Visvesvaraya Technological University (VTU) in 2010. He worked at HCL Technologies Ltd, Bangalore for 3 years from October 2010 - October 2013 in the field of verification and validation. Currently, He is pursing M.Tech in VLSI Design and Embedded systems from Bangalore Institute of Technology, VTU.

Jalaja S holds M.Tech degree in VLSI Design and Embedded System from Visvesvaraya Technological University (VTU). She is a E-Member of IEEE and presently serving as an Assistant Professor in Electronics and Communication Engineering department at Bangalore Institute of Technology, Bangalore (Karnataka). She is currently pursuing the Ph.D. degree in Electronic and Communication engineering from the VTU, Belgaum. Her research interest includes Analysis of various algorithms to design different VLSI architectures and ASIC implementation for digital signal processing applications.