ECC implementation on Nano FPGAs. The proposed ECC cryptoprocessor was modeled using VHDL and synthesized on Actel IGLOO AGLN250V2-VQFP100 Nano FPGA. The synthesis results showed that the targeted Nano FPGA could not exceed the values of $m \leq 11$ bits. This is because of the limited number of resources available on Nano FPGAs. The area result opened a new challenging opportunity for future Nano FPGAs to satisfy the needs of critical portable applications and resource-constrained devices, such as Wireless Sensor Network (WSN).

7. Acknowledgment

The authors would like to acknowledge the support of Umm Al-Qura University, Makkah, Saudi Arabia and the support of LIMOS, CNRS, University Blaise Pascal, Clermont-Ferrand II, France.

8. References

[1] N. Koblitz, Elliptic curve cryptosystems. Math. Comput., Vol. 48, No. 177, pp. 203-209, 1987.

[2] V.S. Miller, "Use of elliptic curves in cryptography", in Proc. of the Advances in Cryptology CRYPTO '85, Springer-Verlag, LNCS 218, pp: 417–426, 1986.

[3] R. 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.

[4] A. Menezes, "Elliptic Curve Public Key Cryptosystems", 1st edition, Kluwer Academic Publishers, 1993.

[5] D. Hankerson, A. Menezes, and S. Vanstone, "Guide to Elliptic Curve Cryptography". 1st edition, Springer, 2004.

[6] C. Paar and J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners". 1st edition, Springer-Verlag, Berlin Heidelberg, 2010.

[7] T. ElGamal,. "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. Advances in Cryptology", in Proc. of CRYPTO 84, August 19-22, Springer Verlag, pp. 10-18, 1985.

[8] D. Hankerson, J.L.Hernandez and A. Menezes, "Software Implementation Of Elliptic Curve Cryptography Over Binary fields. Cryptographic hardware and Embedded Systems", CHES 2000, LNCS 1965, Springer-Verlag, 1-24, 2000.

[9] N. Gura, A. Patel, A. S. Wander, H. Eberle, and S. Chang Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs", in Cryptographic Hardware and Embedded Systems — CHES 2004, vol. 3156 of Lecture Notes in Computer Science, pp. 119-132. Springer Verlag, 2004.

[10] S. Khajuria and H. Tange, "Implementation of diffie-Hellman key exchange on wireless sensor using elliptic curve cryptography", in Proc. 1st International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE '09), pp. 772–776, May 2009.

[11] J. Lutz and A. Hasan, "High performance FPGA based elliptic curve cryptographic co-processor," *in Proc. Int. Conf. Inf. Technol.: Coding Comput. (ITCC),* 2004, p. 486.

[12] G. Meurice de Dormale and J.-J. Quisquater, High-speed hardware implementations of Elliptic Curve Cryptography: A survey. Journal of Systems Architecture: the EUROMICRO Journal, Volume 53, Issue 2-3, pp. 72 – 84, February, 2007.

[13] K. Jarvinen and J. Skytta, On Parallelization of High-Speed Processors for Elliptic Curve Cryptography, *IEEE Trans. on VLSI,* Vol. 16, Issue 9, pp. 1162 – 1175, 2008.

[14] B. Ansari and M. A. Hasan, "High-Performance Architecture of Elliptic Curve Scalar Multiplication", *IEEE Trans. on Computers,* Vol.57, No.11, pp. 1443-1453, 2008.

[15] Kimmo Järvinen, "Optimized FPGA-based elliptic curve cryptography processor for high-speed applications", *Integration, the VLSI Journal,* Volume 44, Issue 4, pp. 270-279, 2011.

[16] Actel IGLOO Nano FPGA Data Sheet, available from: http://www.actel.com/documents/IGLOO_nano_DS.pdf

[17] R. Lidl, and H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University Press, Cambridge, UK, 2nd edition, 1994.

[18] R. C. MULLIN and R. M. WILSON, "Optimal normal bases in $GF(p^n)$", Discrete Appl. Math., 22, pp. 149–161, 1988/1989.

[19] H. Cohen, G. Frey, R.M. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography". Discrete Mathematics and Its Applications, Vol. 34, Chapman and Hall, CRC, USA, 2005.

[20] J.L. Massey and J.K. Omura, "Computational Method and Apparatus for Finite Field Arithmetic," US Patent No. 4,587,627, 1986.

[21] T. F. Al-Somani and A. Amin. "Hardware implementations of $GF(2^m)$ arithmetic using normal basis", J. Appl. Sci., Vol. 6, Issue 6, pp. 1362-1372, 2006.

[22] T. Itoh and S. Tsujii. "A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases", Information and Computation, Vol. 78, pp. 171-177, 1988.

[23] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next Century Challenges: Scalable Coordination in Sensor Networks", in Mobile Computing and Networking (MobiCom'99), Seattle, WA USA (1999) 263–270.

[24] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless Sensor Networks: a survey", Computer Networks, Volume 38, Issue 4, 15 March 2002, Pages 393-422.