Table 3. The x and y input coordinates of the point P and an arbitrary value of k.

k	= 0x 00000001 33E3CAE7 2CD0F448 B2954810 FB75B5E3 D8F43D07
P_x	= 0x 00000003 69979697 AB438977 89566789 567F787A 7876A654
P_y	= 0x 00000004 035EDB42 EFAFB298 9D51FEFC E3C80988 F41FF883

Table 3 show the input parameters of the ECC scalar multiplication for a "163 bits" arbitrary value of k, and in Table 4, we give the implementation results corresponding.

Table 4. Synthesis results for $E(\mathbb{F}_{2^{163}})$.

point multiplication $G(F_{2^{163}})$		
Slice Logic Utilization:		
Number of Slice Registers:	2163	7%
Number of Slice LUTs:	2735	9%
Number used as Logic:	2735	9%
IO Utilization:		
Number of bonded IOBs:	330	58%
Maximum Frequency:	169.477MHz	

In Table 5, we give the implementation results for $\mathbb{F}_{2^{233}}$.

Table 5. Synthesis results for $E(\mathbb{F}_{2^{233}})$.

point multiplication $G(F_{2^{233}})$		
Slice Logic Utilization:		
Number of Slice Registers:	3073	10%
Number of Slice LUTs:	3637	12%
Number used as Logic:	3637	12%
IO Utilization:		
Number of bonded IOBs:	470	83%
Maximum Frequency:	136.323MHz	

8. Conclusion

In this work, the elliptic curve point multiplication is considered, we have analyzed the ECC protocols and designed the ECC processor over the field $GF(2^{163})$. The ECC processor can calculate various operations for implementing ECC protocols, which are a scalar multiplication, an Elliptic Curve point addition, a polynomial multiplication and a polynomial inverse multiplication. It is synthesized and tested with Xilinx FPGA and its average operation frequency for scalar multiplication is 169.477MHz.

9. Acknowledgment

This work was supported by the University of Paris 8.

References

[1] DSS. Digital signature standard (dss). *Federal Information Processing Standards Publication 186-2, National Institute of Standards and Technology*, 2000.

[2] D. H. J. L. Hernandez and A. Menezes. Software implementation of elliptic curve cryptography over binary fields. *In Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems (CHES), volume 1965 of Lecture Notes in Computer Science*, 2001.

[3] IEEE.P1363. Standard specifications for public key cryptography. 2000.

[4] N. Koblitz. Elliptic curve crytosystem. *Mathematics of Computation*, 48:203–209, 1987.

[5] S. S. Kumar. *Elliptic curve cryptography for constrained devices*. PhD thesis, Ruhr-University Bochum, June 2006.

[6] Lejla.BATINA. *Arithmetic and Architectures for Secure Hardware Implementations of Public-Key Cryptography*. PhD thesis, KATHOLIEKE UNIVERSITEIT LEUVEN, December 2005.

[7] D. H. A. Menezes and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[8] V. S. Miller. Use of elliptic curves in cryptography. *Advances in Cryptology - CRYTO '85, Lecture Notes in Computer Science, Springer-Verlag, Hugh C. Williams (Ed.)*, 128:417–426, 1985.

[9] SEC.2. Recommended elliptic curve domain parameters. standard for efficient cryptography. *The SECG Group*, 2000.

