Abstract

Elliptic Curve Cryptography (ECC) has gained increasing acceptance in the industry, the academic community and the cryptography applications. This interest is mainly due to the high level of security with relatively small keys provided by ECC. In this paper, a high-performance ASIC based ECC key generation processor is proposed. This processor supports generic elliptic curves over GF($2^m$) with sizes ($m$) ranging from 113 to 256 bits. The proposed processor is based on programmable cellular automata. For real time implementation, the processor was simulated using active-HDL and synthesized using Synopsys Design Compiler. Further, the processor is implemented by an ASIC CMOS 120 nm technology. The results on the layouted processor over GF($2^{256}$) show a high performance, confirming the efficiency of the processor.
Reference

- M.Morales-Sandoval, C.Feregrino-Uribe, on the hardware design of an elliptic curve cryptosystem, Proceeding of the 5th Mexican International Conference in Computer Science, 2004, pp60-70.
- Dan Young-ping, Zou Xue-cheng, Han Yu and Yi Li-hua, Design of highly efficient elliptic curve crypto-processor with two multiplications over GF(2163), The journal of china Universities of Posts and Telecommunications, Vol 16(2), pp 72-79, 2009.
- M Bednara, M Daldrup, J von zur Gathen and J Shokrollahi, Reconfigurable implementation of elliptic curve crypto algorithms. Reconfigurable Architectures Workshop, 16th International Parallel and Distributed Processing Symposium, April 2002.
High Performances ASIC Based Elliptic Curve Cryptographic Processor over GF(2m)

- A. Daly, W. Maranane, T. Kerins and E. Popocivi, "Fast Modular Division for Application in ECC on Reconfiguration Logic”, Field Programmable Logic and application, 13th International Conference, (FPL '03),2003, pp. 786-795.
- E. Oswald, "Introduction to elliptic curve Cryptography", Institute for Applied information Processing and communication, July 2005. 2

Index Terms

Computer Science Security
Key words

Elliptic curve cryptography

cellular automata

finite fields

ASIC

Montgomery point multiplication algorithm