Fast Elliptic Curve Cryptographic Processor Architecture Based On Three Parallel GF(2/Sup K/) Bit Level Pipelined Digit Serial Multipliers

Gutub, A.A.-A.; Dept. of Comput. Eng., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia;

Electronics, Circuits and Systems, 2003. ICECS 2003. Proceedings of the 2003 10th IEEE International conference;Publication Date: 14-17 Dec. 2003;Vol: 1,On page(s): 72- 75 Vol.1;ISBN: 0-7803-8163-7

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

Unusual processor architecture for elliptic curve encryption is proposed in this paper. The architecture exploits projective coordinates (x=X/Z, y=Y/Z) to convert GF(2/sup k/) division needed in elliptic point operations into several multiplication steps. The processor has three GF(2/sup k/) multipliers implemented using bit-level pipelined digit serial computation. It is shown that this results in a faster operation than using fully parallel multipliers with the added advantage of requiring less area. The proposed architecture is a serious contender for implementing data security systems based on elliptic curve cryptography.