High Radix Parallel Architecture For GF(P) Elliptic Curve Processor

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

Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03). 2003 IEEE International conference;Publication Date: 6-10 April 2003;Vol: 2, On page(s): II- 625-8 vol.2;ISBN: 0-7803-7663-3

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

A new GF(p) cryptographic processor architecture for elliptic curve encryption/decryption is proposed in this paper. The architecture takes advantage of projective coordinates to convert GF(p) inversion needed in elliptic point operations into several multiplication steps. Unlike existing sequential designs, we show that projecting into (X/Z,Y/Z) leads to a much better performance than the conventional choice of projecting into the current (X/Z/sup 2/,Y/Z/sup 3/). We also propose to use high radix modulo multipliers which give a wide range of area-time trade-offs. The proposed architecture is a significant challenger for implementing data security systems based on elliptic curve cryptography.