

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

Gutub, AAA; Ibrahim, MK

I E E E, 2003 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH, AND SIGNAL

PROCESSING, VOL II, PROCEEDINGS - SPEECH II; INDUSTRY TECHNOLOGY TRACKS; DESIGN IMPLEMENTATION OF SIGNAL PROCESSING SYSTEMS; NEURAL

NETWORKS FOR SIGNAL PROCESSING; pp: 625-628; Vol: ##

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 improved performance than conventional choice of projecting into the current $(X/Z(2), Y/Z(3))$. 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.

References:

1. BLAKE, 2000, ELLIPTIC CURVES CRYPT
2. CHUNG S, 2000, WORKSH CRYPT HARDW E
3. CRUTCHLEY DA, 1999, THESIS U SOUTHAMPTON
4. ERCEGOVAC MD, 1999, INTRO DIGITAL SYSTEM
5. HANKERSON, 2000, WORKSH CRYPT HARDW E
6. MEKHALLALATI MC, 1996, J CIRCUIT SYST COMP, V6, P547
7. MIYAJI A, 1992, ADV CRYPTOLOGY AUSCR
8. OKADA, 2000, WORKSH CRYPT HARDW E
9. ORLANDO, 2000, WORKSH CRYPT HARDW E

© Copyright: King Fahd University of Petroleum & Minerals;
<http://www.kfupm.edu.sa>

10. ORLANDO, 2001, CRYPTOGRAPHIC HARDWA
11. ORTON GA, 1987, LECT NOTES COMPUTER, V263, P277
12. PAAR, 1999, IEEE T COMPUTERS, V48
13. SCOTT NR, 1985, COMPUTER NUMBER SYST
14. STALLINGS W, 1999, CRYPTOGRAPHY NETWORK
15. STINSON DR, 1995, CRYPTOGRAPHY THEORY
16. TOCCI RJ, 2001, DIGITAL SYSTEMS PRIN

For pre-prints please write to: abstracts@kfupm.edu.sa