Journal of Signal Processing Systems, Springer
The original publication is available at: www.springerlink.com

Efficient FPGA Implementation of a Programmable Architecture for GF(p) Elliptic Curve Crypto Computations

Lo’ai Tawalbeh, Abidalrahman Mohammad, Adnan Gutub

Lo’ai Tawalbeh and Abidalrahman Mohammad are with
Computer Engineering Department, Jordan University of Science and Technology, Irbid, Jordan
Email: tawalbeh@just.edu.jo, abdmoh@gmail.com

Adnan Gutub is with
Computer Engineering Department
King Fahd University of Petroleum & Minerals, Dhahran 31261, Saudi Arabia
Email: gutub@kfupm.edu.sa

ABSTRACT

This paper presents a processor architecture for elliptic curve cryptography computations over GF(p). The speed to compute the Elliptic-curve point multiplication over the prime fields GF(p) is increased by using the maximum degree of parallelism, and by carefully selecting the most appropriate coordinates system. The proposed Elliptic Curve processor is implemented using FPGAs. The time, area and throughput results are obtained, analyzed, and compared with previously proposed designs showing interesting performance and features.

KEYWORDS

cryptography hardware, modular arithmetic, security architecture, design