Abstract

This paper proposes the implementation of a Elliptic Curve (EC) cryptosystem which is aimed to provide secure stream ciphers, hash functions and key exchange in a time shared manner. The design of hardware efficient stream cipher based on elliptic curves proposes the use of point multiplication block on a time sharing basis for providing secure stream ciphers, hash generation and key exchange. The EC point multiplication uses the Gaussian normal bases for field arithmetic. The designs were implemented using Verilog language and the hardware implementation was done using a Field Programmable Gate Array (FPGA) device.
Signatures and Public-Key Cryptosystems, Communications of the ACM.
Index Terms

Computer Science  Security

Keywords

Hash function  Elliptic curve cryptosystems  Stream cipher  Gaussian normal  basis

Finite fields

FPGA