World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:8, No:12, 2014

# Implementation of Elliptic Curve Cryptography Encryption Engine on a FPGA

**Authors :** Mohamad Khairi Ishak

**Abstract :** Conventional public key crypto systems such as RSA (Ron Rivest, Adi Shamir and Leonard Adleman), DSA (Digital Signature Algorithm), and Elgamal are no longer efficient to be implemented in the small, memory constrained devices. Elliptic Curve Cryptography (ECC), which allows smaller key length as compared to conventional public key crypto systems, has thus become a very attractive choice for many applications. This paper describes implementation of an elliptic curve cryptography (ECC) encryption engine on a FPGA. The system has been implemented in 2 different key sizes, which are 131 bits and 163 bits. Area and timing analysis are provided for both key sizes for comparison. The crypto system, which has been implemented on Altera's EPF10K200SBC600-1, has a hardware size of 5945/9984 and 6913/9984 of logic cells for 131 bits implementation and 163 bits implementation respectively. The crypto system operates up to 43 MHz, and performs point multiplication operation in 11.3 ms for 131 bits implementation and 14.9 ms for 163 bits implementation. In terms of speed, our crypto system is about 8 times faster than the software implementation of the same system.

**Keywords :** elliptic curve cryptography, FPGA, key sizes, memory
**Conference Title :** ICCINS 2014 : International Conference on Communications, Information and Network Security
**Conference Location :** Sydney, Australia
**Conference Dates :** December 15-16, 2014