FPGA Implementation of Low Power and High Speed Hummingbird Cryptographic Algorithm

Abstract

Hummingbird is the latest ultra-lightweight cryptographic algorithm targeted for low cost smart devices. In this paper, we design a low power and high speed lightweight cryptographic Hummingbird algorithm for hardware environment. The performance of the approach used is determined on XILINX platform using Verilog as hardware description language. We have used Verilog for designing as well as simulation purposes. To verify digital design at the software platform we used ModelSim 6. 2b simulator and XILINX 9. 2i ISE suite is the synthesis tool used to transform design into digital circuits. An enhanced FPGA implementation of the Hummingbird cryptographic algorithm for low power and high operating speed (with max frequency) is performed using Virtex5 family of XILINX ISE suite. Comparisons to the other reported FPGA implementations of the Hummingbird, our proposed design outperforms the previous work in terms of speed and power requirements.

References

FPGA Implementation of Low Power and High Speed Hummingbird Cryptographic Algorithm


**Index Terms**

Computer Science  Security

**Keywords**

Hummingbird Cryptographic Algorithm  Lightweight Cryptography  Constrained devices  FPGA