Abstract

The Efficiency of present symmetric encryption algorithms mainly depends on implementation cost and resulting performances. Present symmetric encryption, like the Advanced Encryption Standard (AES) rather focus on finding a good tradeoff between cost, security and performances. Some present symmetric encryption algorithms are targeted for software implementations and shows significant efficiency improvements on these platforms compared to other algorithms. From these algorithms, consider a general context where we have very limited processing resources (e.g. a small processor). It yields design criteria such as: low memory requirements, small code size, limited instruction set, i.e. Scalable Encryption Algorithm (SEA). For this purpose, loop architecture of the block cipher is presented. The total modules of SEA written in VHDL coding, the simulation and synthesis results are verified by the Virtex-4 of Xilinx 9.1i. This paper also carefully describes the implementation details and corresponding area requirements.

References

- Rao, K. D.; Gangadhar, C. VLSI realization of a secure cryptosystem for image encryption and decryption Communications and Signal Processing (ICCSP), 2011 IEEE International Conference 2011, Page(s): 543 - 547
- Dam J. Elbirt, "Reconfigurable Computing for Symmetric-Key Algorithms".


- A. Menezes, P. van, "Handbook of Applied Cryptography".

- Hongyong Jia; Yue Chen; Xiuqing Mao; Ruiyu Dou Efficient and scalable multicast key management using attribute based encryptionv Information Theory and Information Security (ICITIS), 2010 IEEE International Conference 2010, Page(s): 426 - 429


- Jiang Bian; Seker, R. ; Topaloglu, U. ; Bayrak, C. A scalable Role-based Group Key Agreement and Role Identification mechanism Systems Conference (SysCon), 2011 IEEE International 2011, Page(s): 278 - 281

Index Terms

Computer Science Security

Keywords

Block Cipher Sea