Abstract

This work reports Partial Reconfiguration (PR) by which selected areas of an FPGA can be reconfigured during runtime. Today cryptographic algorithms are not safe also embedded cryptographic hardware is costly. Hence to make it cost effective and to provide more secureness reconfigurable hardware such as FPGA is used with the concept of partial reconfiguration. This work gives briefings about the method of hardware implementation for AES encryption algorithm with Dynamic reconfigurable keys. Our implementation reaches very good efficiencies than the compared one as we have adopted our own methodology for key expansion. With the combination of adopted methodology & used FPGA this paper shows better agreement as compared to previous work. This implementation could be a good solution to preserve confidentiality and convenience to the information in the numeric communication.

References

Dynamic Partial Reconfiguration Implementation of AES Algorithm

- Jose M. Granado-Criado, Miguel A. Vega-Rodr?ez, Juan M. Sanchez-Perez, Juan A. Gomez-Pulido, "A new methodology to implement the AES algorithm using partial and dynamic reconfiguration," in INTEGRATION, the VLSI journal 43(2010).
Index Terms

Computer Science
Security

Keywords

Partial Reconfiguration  Embedded system  Reconfigurable computing
cryptography
FPGA