II-O-1.1

AN EMBEDDED ARIA FOR WIRELESS NETWORK APPLICATIONS

Deng Lin, Kyu-Kwan Kim, Seung-Youl Kim, Younggap You[1]
[1]Department of Information and Communication Engineering
Chungbuk National University, Korea

Abstract

This paper discusses performance enhancement of single core architecture of a block cipher system, named ARIA which is based on involutional substitution and permutation. The proposed architecture employs two sets of pipeline stages: one set comprising pipeline stages for the S-box layer, and one set for pipeline stages in the permutation layer. Substantial circuit size reduction has been achieved through merging of the shift rows and inverse shift rows by sharing the same resources by mix column and inverse mix column functions. The proposed architecture has been implemented in Verilog HDL, and yields 400 Mbits/s throughput on the 0.18um CMOS process technology. This high performance architecture can enhance security capability of wireless network systems.

Key words: cryptographic processor, ARIA, embedded system, network router.