RC4A stream cipher for WLAN security: a hardware approach

ABSTRACT

Wireless networks are on the cutting edge of modern technology and rapidly gaining popularity in todayôs world due to their excellent usability. For secure wireless data transmission, Wired Equivalent Privacy (WEP), IEEE 802.11 standard defined security protocol, is employed. WEP has a potential limitation that stems from its adaptation of RC4 stream cipher algorithm. As a result, there is a pressing need for new WLAN security measure. Therefore, this paper presents hardware implementation of RC4A stream cipher and proposes to replace RC4 in WLAN security scheme, due to weakness of RC4.The design of the cipher was implemented by Verilog HDL. For hardware implementation of the design, an Altera Field Programmable Gate Array (FPGA) device, EP20K200EFC484-2X from APEX family, APEX 20KE, was used.