World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:17, No:07, 2023

PUF-Based Lightweight Iot Secure Authentication Chip Design

Authors : Wenxuan Li, Lei Li, Jin Li, Yuanhang He

Abstract : This paper designed a secure chip for IoT communication security integrated with the PUF-based firmware protection scheme. Then, the Xilinx Kintex-7 and STM-32 were used for the prototype verification. Firmware protection worked well on FPGA and embedded platforms. For the ASIC implementation of the PUF module, contact PUF is chosen. The post-processing method and its improvement are analyzed with emphasis. This paper proposed a more efficient post-processing method for contact PUF named SXOR, which has practical value for realizing lightweight security modules in IoT devices. The analysis was carried out under the hypothesis that the contact holes are independent and combine the existing data in the open literature. The post-processing effects of SXOR and XOR are basically the same under the condition that the proposed post-processing circuit occupies only 50.6% of the area of XOR. The average Hamming weight of the PUF output bit sequence obtained by the proposed post-processing method is 0.499735, and the average Hamming weight obtained by the XOR-based post-processing method is 0.499999.

Keywords : PUF, IoT, authentication, secure communication, encryption, XOR
Conference Title : ICSLP 2023 : International Conference on Speech and Language Processing
Conference Location : Stockholm, Sweden
Conference Dates : July 06-07, 2023