سیویلیکا - ناشر تخصصی مقالات کنفرانس ها و ژورنال ها
گواهی ثبت مقاله در سیویلیکا
CIVILICA.com

عنوان مقاله:

Lightweight Structure of Random Key Generation for PRESENT Block Cipher

محل انتشار:

مجله الکترونیک صنعتی ،کنترل و بهینه سازی, دوره 7, شماره 1 (سال: 1403)

تعداد صفحات اصل مقاله: 11

نویسنده:

Bahram Rashidi - Dept. of Elec. Eng., Ayatollah Boroujerdi University

خلاصه مقاله:

In this paper, we design a lightweight and modified random key generation for PRESENT block cipher which is applicable in the encryption of the digital signals. In the block ciphers, the master key is used directly in the encryption process for the data (plaintext). But in this work, a master key (initial key) is used to derive the new random master keys (random session keys) and use these keys for the encryption process. The use of random keys will overcome the brute force attack that can be applied to the PRESENT cipher. The random session keys generated will produce different ciphertexts for the same plaintext for every session. In this approach, we take advantage of the block cipher to produce random keys. The PRESENT cipher is shared in both random key generation and encryption process. Therefore, the proposed structure has both random key generation and data encryption in a unified circuit. This property reduces hardware resources. The implementation results, in ۱۸۰ nm CMOS technologies, show the proposed structure is comparable in terms of area and .delay with other works

کلمات کلیدی:

PRESENT block cipher, Random key generation, Lightweight, High-throughput, ASIC

لینک ثابت مقاله در پایگاه سیویلیکا:

https://civilica.com/doc/1950721