https://ieeexplore.ieee.org/document/8640941

NVLC: New Variant Lightweight Cryptography Algorithm for Internet of Things

Seddiq Abd Al-Rahman; Ali Sagheer; Omar Dawood

Abstract:

The rapid industrial and technological development along with the continues need to improve lifestyle have led to the emergence of the Internet of Things (IoT) as a service. Due to its nature, there are a huge amount of data been transmitted over IoT in every minute. Considering security aspects of such a huge data, with limited resources including bandwidth and energy, requires an innovative way of securing such as data driven environment. This study aims to propose a low-cost encryption algorithm (NVLC) to handle a low-cost Radio-frequency Identification (RFID) tags and sensors within IoT environment. NVLC is a symmetric block cipher with a 64-bit block size data and 80-bit/128-bit for the secret key. Although 6 rounds of NVLC is enough to maintain data security, however, we are applying 20 rounds to increase data security and complexity of decryption. This paper uses a substitution-permutation network within NVLC as a uniform architecture of cryptography. NVLC has been designed and implemented using a combination of mathematical and logical and methods considering the requirement of IoT lightweight devices and infrastructure. The proposed cipher was shown the security evaluation, software, and hardware experiments to it, and results show that compares to other lightweight block ciphers. NVLC has an advantage in the term used low cost of gate equivalents (GE), used only 1134GE.

Published in: 2018 1st Annual International Conference on Information and Sciences (AiCIS)

Date of Conference: 20-21 Nov. 2018

Date Added to IEEE *Xplore*: 14 February 2019

ISBN Information:

INSPEC Accession Number: 18468678

DOI: 10.1109/AiCIS.2018.00042

Publisher: IEEE

Conference Location: Fallujah, Iraq

Keywords

Ciphers, Encryption, Germanium, Internet of Things, Hardware