A Study on Transmission Overhead of Post Quantum Cryptography Algorithms in Internet of Things Networks

Mahmoud AbdelHafeez, Mohamed M. Abdelraheem, Mostafa I. Taha, Elsayed Esam M. Khaled

Abstract:

Post-quantum cryptography is an emerging solution to the expected security breach, introduced by quantum computers, to the currently used public key cryptosystems. This paper presents an experimental study on the effect of the overhead associated with the wireless transmission of some of the newly developed post quantum cryptography algorithms through the Internet of Things networks. Experimental results of this work include the energy and time measurements for wireless transmission of chosen sample messages of these new cryptographic algorithms. In addition, recommendations are given for appropriate modules configurations and choice of suitable security algorithm for the Internet of Things networks.

Keywords:

IoT Security, Post Quantum Cryptography, Wi-Fi

Published In:

2019 31st International Conference on Microelectronics (ICM2019), NULL, 113-117