Paper ID 2012

Statistical Comparison of Grain Algorithm for IoT Device Security

Ari Kusyanti, Rakhmadhany Primananda, Adhitya Bhawiyuga, Ajeng Nurrohmah
Faculty of Computer Science
University of Brawijaya
Malang, Indonesia
ari.kusyanti@ub.ac.id, rakhmadhany@ub.ac.id, bhawiyuga@ub.ac.id, ajeng.nurrohmah@ub.ac.id

***Abstract*— Internet of Things (IoT) is an interconnection among devices or "things" that exchange data between them. A man-in-the-middle can be performed when two IoT devices are communicating, therefore secure data transmission between IoT devices has emerged as a challenging task. There are numbers of existing cryptography algorithms that offers protection. However, their utilization in IoT is questionable since the hardware is not suitable for inexpensive yet efficient encryption process. This paper proposed implementation of Grain as the winner for eSTREAM project and compare all version of Grain, i.e Grain v0, Grain v1 and Grain 128 in Arduino Mega 2560 as it used as a single board computer for IoT. The result shows that there is no significant difference in encryption-decryption processing time. While, in generating keystream, Grain 128 will take more time when implemented in Arduino Mega 2560.**

Keywords—internet of things; cryptography; grain algorithm; Arduino Mega 2560