Enhancing speed of SIMON: A lightweight-cryptographic algorithm for IoT applications

Norah Alassaf, Adnan Gutub, Shabir A. Parah & Manal Al Ghamdi

Multimedia Tools and Applications
An International Journal
ISSN 1380-7501
Multimed Tools Appl
DOI 10.1007/s11042-018-6801-z
Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications

Norah Allassaf1 · Adnan Gubit1 · Shabir A. Parah2 · Manal Al Ghamdi3

Received: 11 April 2018 / Revised: 13 October 2018 / Accepted: 23 October 2018
Published online: 05 November 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
Multimedia communication is revolutionizing all major spheres of human life. The advent of IoT and its applications in many fields like sensing, healthcare and industry, result exponential increase in multimedia data, that needs to be shared over insecure networks. IoT driven setups are however constrained in terms of resources as a result of their small size. From data security point of view a conventional algorithms cannot be used for data encryption on an IoT platform given the resource constraints. The work presented in this paper studies the performance of SIMON cryptographic algorithm and proposes a light-weight-cryptography algorithm based on SIMON for its possible use in an IoT driven setup. The focus is on speed enhancement benefitting from software prospective, making it different than common studies mostly reflecting hardware implementations. To achieve performance in practical prospective, the contribution looks into SIMON cipher’s characteristics considering utilizing it for internet of things (IoT) healthcare applications. The paper suggests further improvement to implement the original SIMON cryptography in order to reduce the encryption time and maintain the practical trade-off between security and performance. The proposed work has been compared to Advanced Encryption Standard (AES) and the original SIMON block cipher algorithms in terms of execution time, memory consumption. The results show that the proposed work is suitable for securing data in an IoT driven setup.

Keywords Internet of things · Medical data · AES · SIMON cipher · Light weight cryptography

Shabir A. Parah
shabirehr@gmail.com

1 Department of Computer Engineering, Umm Al-Qura University (UQU), Makkah, Saudi Arabia
2 Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, JK, India
3 Department of Computer Sciences, Umm Al-Qura University, Makkah, Saudi Arabia