3rd International Conference on Engineering Technology and Applied Sciences

17-21 July 2018
Skopje / MACEDONIA

www.icetas.com

Book of Abstracts

ISBN: 978-605-4444-12-0


Edited by Assoc. Prof. Dr. Ayhan EROL
Asist. Prof. Dr. Ahmet YÖNETKEN
Published Afyon Kocatepe University, 2018
info@icetas.com
3rd International Conference on Engineering Technology and Applied Sciences

ICETAS 2018
Skopje/Macedonia 17-21 July 2018
www.icetas.com
Book of Abstracts

ISBN:978-605-4444-12-0

Book of Abstracts of the International Conference on Engineering Technology and Applied Sciences
(ICETAS 2018)

Edited by Assoc. Prof. Dr. Ayhan EROL
Asist. Prof. Dr. Ahmet YÖNETKEN

Published Afyon Kocatepe University, July 2018,
info@icetas.com

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned. Nothing from this publication may be translated, reproduced, stored in a computerized system or published in any form or in any manner, including, but not limited to electronic, mechanical, reprographic or photographic, without prior written permission from the publisher www.icetas.com yonetken@aku.edu.tr The individual contributions in this publication and any liabilities arising from them remain the responsibility of the authors. The publisher is not responsible for possible damages, which could be a result of content derived from this publication.
A HYBRID RANDOM NUMBER GENERATOR FOR LIGHTWEIGHT CRYPTOSYSTEMS: XORSHIFTLPLUS

ÖMER AYDIN\textsuperscript{a}, GÖKHAN DALKILIÇ\textsuperscript{b}

\textsuperscript{a}FACULTY OF ECONOMICS AND ADMINISTRATIVE SCIENCES, DOKUZ EYLÜL UNIVERSITY
\textsuperscript{b}COMPUTER ENGINEERING DEPARTMENT, FACULTY OF ENGINEERING, DOKUZ EYLÜL UNIVERSITY

omer.aydin@deu.edu.tr

Abstract:

Lightweight devices such as radio frequency identification tags, smart cards, wireless sensor nodes and devices belong to Internet of Things concept continue to grow day by day, so there exists a serious need for effective and lightweight security structures for them. In this paper, an effective and lightweight pseudo random number generator seeded by the non-random hardware source is proposed. Built-in temperature sensor is used to seed the lightweight pseudo random number generator as a hardware source. The proposed hybrid generator is built on the structure of xorshift. This generator is ultralight version of xorshift with fewer number of shift, XOR operations and the short bit length of the seeds. The new and lightweight generator is called the xorshiftLplus in which “L” stands for “lightweight”, demonstrated great suitability for lightweight devices considering its randomness, performance and resource usage. This random number generator is tested for the three EPC\textsuperscript{TM} Gen-2 Class 1 conditions that is mentioned in EPC\textsuperscript{TM} Gen-2 Class 1 document and with NIST randomness test suite. It is implemented on WISP passive RFID tag to investigate time and resource usage.

Keywords: Xorshift, Lightweight Hybrid Random Number Generator, Internet Of Things, WISP, Nist

\textsuperscript{*}This study is supported by The Scientific & Technological Research Council of Turkey (TUBITAK) with the project number 215E225.