International Conference on Information and Communication Technology and Applications ICTA 2020: pp 415-429|

Sooner Lightweight Cryptosystem: Towards Privacy Preservation of Resource-Constrained Devices

- Abraham Ayegba Alfa
- John Kolo Alhassan
- Olayemi Mikail Olaniyi
- Morufu Olalere

Part of the Communications in Computer and Information Science book series (CCIS, volume 1350)

Abstract

The use of cryptosystem became popular because of the increased need for exchanges across untrusted medium especially Internet-enabled networks. On the basis of application several forms of cryptosystems have been developed for purpose of authentication, confidentiality, integrity, and non-repudiation. Cryptosystems make use of encryption schemes that convert plaintext to ciphertext in diverse areas of applications. The vast progressions in the Internet of Things (IoT) technology and resource-constrained devices have given rise to massive deployment of sensor devices and growth of services targeted at lightweight devices. Though, these devices support a number of services, they require strong lightweight encryption approaches for privacy protection of data. Existing lightweight cryptosystems fall short on the expected privacy levels and applicability in emerging resource-constrained environment. This paper develops a mathematical model for a Sooner lightweight cryptographic scheme based on reduced and hardened ciphertext block sizes, hash sizes and key sizes of traditional cryptosystems and Public Blockchain technology for ubiquitous systems. Thereafter, the hardening procedure offered by the RSA homomorphic encryption was applied for the purpose of generating stronger, secure and lightweight AES, RSA and SHA-3 in order to deal with untrusted channels exchanges. The proposed Sooner is recommended for adoption in public Blockchain-based smart systems and applications for the purpose of data privacy.

Keywords

Lightweight cryptosystem Block size Key size Resource-constrained devices Hashes Hardening

https://link.springer.com/chapter/10.1007%2F978-3-030-69143-1_32