

CRYPTOGRAPHIC TECHNIQUES FOR IOT DEVICES: A SURVEY

Fernando Ramirez Arredondo
School of Computer Science
Universidad Católica San Pablo
Email: fernando.ramirez@ucsp.edu.pe

Abstract—Lightweight Cryptography (LWC) is an expanding field of research as a result of its importance in securing IoT devices and other systems where traditional cryptography would be impractical due to their resource demands. It is for this reason that several LWC primitives have been proposed, with lightweight block ciphers being the most popular in terms of methods proposed and usage. This work surveys lightweight block ciphers' algorithms for resource-constrained devices, which have become increasingly important in today's world for their wide range of useful applications, from convenience and efficiency in our daily routines to far-reaching applications in healthcare, industry, and urban planning. The goal of this work is to provide a comprehensible classification of these methods in terms of performance and resources required, followed by an accurate explanation of the tradeoff between these two when working with limited resources.

Index Terms—Lightweight cryptography (LWC), Lightweight block ciphers, Resource-constrained devices

<https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>, accessed: 2023-11-07.

1. Introduction

Back in 2016, World Economic Forum founder and executive chairman Klaus Schwab wrote a book titled *The Fourth Industrial Revolution*, in which he explained that the way we live, work and relate to one another was about to be fundamentally altered by a digital revolution unlike the ones humanity had experienced before. Back to today, this so-called fourth industrial revolution has been characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres [1].

2. Theoretical framework

3. Related Work

4. Taxonomy

5. Strengths and Weaknesses

6. Conclusions

References

- [1] "World Economic Forum the fourth industrial revolution: what it means, how to respond,"