Securing Data in Low-Resource Systems: Lightweight Block Cryptography Strategies

Fernando Ramirez Arredondo
dept. name of organization (of Aff.)
name of organization (of Aff.)
Arequipa, Perú
fernando.ramirez@ucsp.edu.pe

Yván Jesús Túpac Valdivia
dept. name of organization (of Aff.)
name of organization (of Aff.)
Arequipa, Perú
ytupac@ucsp.edu.pe

***Abstract*—Aquí deberá colocar el abstract del trabajo en español. No debe modificar el formato de este documento, decir, no debe cambiar ni el tipo ni el tamaño de la fuente. No debe cambiar el ancho de los márgenes. No debe cambiar el interlineado, etc.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introducción

Aquí deberá colocar la introducción del paper. Debe incluir un contexto (situar el tema), la descripción de un problema, el objetivo y la organización del texto. Esta sección no debe tener subsecciones. La descripción debe seguir la descripción en embudo, es decir de los más general a lo más específico.

II. Estado del Arte

Aquí deberá colocar el estado del arte de la investigación. En el estudio de Fan et al. [1], se definió un cifrado ligero como un algoritmo criptográfico diseñado específicamente para dispositivos con recursos limitados. El algoritmo necesitaba abordar tres desafíos clave: minimizar la sobrecarga (en términos de área de silicio o huella de memoria), garantizar un bajo consumo de energía y mantener un nivel suficiente de seguridad.

Otros investigadores han adoptado un enfoque cuantitativo para la definición de cifrados ligeros. Por ejemplo, en el estudio realizado por Cazorla et al. [2] se propusieron criterios específicos para categorizar un cifrado como ligero. Estos criterios abarcan atributos como el tamaño del bloque, el tamaño de la clave, las operaciones y la programación de claves. En el contexto de los cifrados de bloque ligeros, el término ”ligero” denota un tamaño de bloque reducido (32, 48 o 64 bits) en contraste con los cifrados convencionales, que suelen tener tamaños de bloque más grandes (64 o 128 bits).

El informe NIST IR 8114 [3], trabajando hacia la estandarización de estos algoritmos, define la criptografía ligera como un subcampo de la criptografía que tiene como objetivo proporcionar soluciones adaptadas para dispositivos con recursos limitados.

III. Técnicas para resolver el problema

Aquí deberá dar la descripción detallada de las técnicas que va a comparar y que por lo tanto va a implementar. Deberá crear dos secciones, una para cada técnica.

A. Substitution-Permutation Network

B. Feistel Network

IV. Experimentos y Resultados

En esta sección debe colocar los experimientos y resultados. Si el proyecto todavía no tiene resultados, debe eliminar esta sección.

V. Conclusiones

Aquí debe colocar las conclusiones

References

[1] X. Fan, K. Mandal, and G. Gong, “Wg-8: A lightweight stream cipher for resource-constrained smart devices,” in *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 9th International Conference, QShine 2013, Greader Noida, India, January 11-12, 2013, Revised Selected Papers 9*. Springer, 2013, pp. 617–632.

[2] M. Cazorla, K. Marquet, and M. Minier, “Survey and benchmark of lightweight block ciphers for wireless sensor networks,” in *2013 international conference on security and cryptography (SECRYPT)*. IEEE, 2013, pp. 1–6.

[3] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, “Report on lightweight cryptography,” National Institute of Standards and Technology, Tech. Rep., 2016.