MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2025-2026

PROPUESTA

Título:	*Diseño e implementación hardware del cifrador de bloque para criptografía ligera LED*
Título en inglés:	*Design and hardware implementation of LED block cipher*
Tutor/es:	*José Luis Imaña Pascual (DACyA)*
Correos-e:	*jluimana@ucm.es*
Lugar de realización:	Facultad Ciencias Físicas, despacho 226.0

Resumen:

El cifrador de bloque LED (*Lightweight Encryption Device*) es un algoritmo diseñado específicamente para criptografía ligera, orientado a dispositivos con recursos limitados como sensores, etiquetas RFID o sistemas empotrados. Su estructura se basa en una red de sustitución-permutación (SPN) con operaciones sencillas que reducen el consumo de energía y área en hardware, manteniendo un nivel adecuado de seguridad. LED utiliza bloques de 64 bits y claves de 64, 80 o 128 bits, equilibrando seguridad y eficiencia para aplicaciones IoT (Internet de las Cosas).

LED está basado en los principios de diseño de AES (*Advanced Encryption Standard*) y utiliza operaciones compactas como rotaciones, sumas módulo 4 y sustituciones mediante S-boxes de 4 bits, que permiten implementaciones con un número reducido de puertas lógicas. La simplicidad de sus rondas facilita una arquitectura eficiente en área, logrando que incluso dispositivos de muy bajo coste puedan implementar un cifrado seguro. Además, la implementación hardware de LED en diferentes plataformas ha mostrado que puede ofrecer un compromiso favorable entre consumo energético, área ocupada y rendimiento, convirtiéndose en una alternativa viable para proteger comunicaciones en sistemas empotrados donde algoritmos como AES resultan demasiado costosos. De esta manera, LED se consolida como un referente en el campo de la criptografía ligera, ofreciendo seguridad eficiente en plataformas con recursos altamente restringidos.

En este trabajo se estudiará el cifrador de bloque LED para criptografía ligera y se propondrán diferentes arquitecturas que serán descritas en un lenguaje de descripción hardware e implementadas en una FPGA de Xilinx, empleando para ello las herramientas de diseño adecuadas. La comparación de los resultados obtenidos para las distintas descripciones implementadas permitirá determinar la mejor arquitectura.

Metodología:

El trabajo constará de las siguientes tareas:

- Adquisición de los conocimientos previos necesarios sobre criptografía clásica y el cifrado por bloque.
- Comprensión del funcionamiento del cifrador de bloque LED.
- Aprendizaje del lenguaje de descripción hardware VHDL y de las herramientas de diseño adecuadas.
- Descripción en VHDL e implementación sobre FPGA de distintas arquitecturas correspondientes al cifrador LED.
- Comparación y análisis de los resultados obtenidos

Conocimientos previos recomendados:

- Conocimientos de programación en lenguajes de alto nivel.

Bibliografía:

- J. Guo, T. Peyrin, A. Poschmann, M. Robshaw. The LED Block Cipher. Conference on Cryptographic Hardware and Embedded Systems CHES 2011, LNCS 1917, pp. 326-341, 2011.
- A. Mhaouch, W. Gtifa, A. Abdeali, A. Sakly, M. Machhout. Design and hardware implementation of LED block cipher for vehicles keyless entry systems. Egyptian Informatics Journal, 30(2025) 100687, pp. 1-16, abril 2025.
- A. Mhaouch, W. Ayadi, S. Ridha, K. Issa, A.B. Abdelali, M. Machhout. An efficient hardware implementation of LED lightweight block cipher. 7th IEEE International Conference on Advanced Technologies, Signal and Image Processing (ATSIP2024), pp. 312-316, julio 2024.