UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

Propuesta TFG. Curso 2024/2025

GRADO: Grado en Ingeniería Electrónica Industrial

CÓDIGO DEL TFG: 205-041-2024/2025

1. DATOS BÁSICOS DEL TFG:

Título: Implementación Hardware de un criptosistema ligero basado en Ascon

Descripción general (resumen y metodología):

El despliegue y la utilización de dispositivos IoT en cada vez más ámbitos, incluidos los relacionados con la Industria y las aplicaciones militares hacen necesario dotarlos de unos niveles de seguridad adecuados mediante sistemas criptográficos. Por otra parte, las restricciones en los recursos disponibles en este tipo de dispositivos dificultan el uso de los algoritmos criptográficos usuales, lo que ha llevado a los organismos internacionales como el NIST a abordar la estandarización de la denominada criptografía ligera. Así, recientemente dicho organismo ha adoptado la familia de algoritmos ASCON como estándar para criptografía ligera. En este trabajo se propone la implementación hardware en FGPAs de bajo coste de esta familia de algoritmos, con el fin de asegurar dispositivos IoT realizados sobre dispositivos reconfigurables.
Para llevar a cabo el trabajo se seguirá la siguiente medología:

- Revisión de la documentación de ASCON
- Estudio de las librerías software existentes sobre ASCON en Python
- Traslado del algoritmo software a VHDL
- Implementación en FPGA de ASCON
- Verificación del funcionamiento del core desarrollado.

Tipología: Trabajos experimentales, de toma de datos de campo o de laboratorio.

Objetivos planteados:

Los principales objetivos del TFG son:

- Comprensión del conjunto de algoritmos que conforman ASCON
- Saber utilizar las librerías software de ASCON
- Realizar un core en FPGA capaz de realizar las operaciones requeridas por ASCON

Bibliografía básica:

- Lloris, Prieto, Parrilla: "Sistemas digitales", McGraw Hill, 2006
- Short: "VHDL for engineers (New International Edition)", Pearson, 2013
- ASCON NIST submission, https://ascon.iaik.tugraz.at/files/asconv12-nist.pdf

Recomendaciones y orientaciones para el estudiante:

Se recomienda tener conocimientos de VHDL y programación (preferiblemente Python).

Plazas: 1

2. DATOS DEL TUTOR/A:

Nombre y apellidos: LUIS PARRILLA ROURE

Ámbito de conocimiento/Departamento: ELECTRÓNICA

Correo electrónico: luis@ugr.es

3. COTUTOR/A DE LA UGR (en su caso):

Nombre y apellidos: MARÍA ENCARNACIÓN CASTILLO MORALES

Ámbito de conocimiento/Departamento: ELECTRÓNICA

Correo electrónico: encas@ugr.es

4. COTUTOR/A EXTERNO/A (en su caso):

Nombre y apellidos:

Correo electrónico:

Nombre de la empresa o institución:

Dirección postal:

Puesto del tutor en la empresa o institución:

5. DATOS DEL ESTUDIANTE:

Nombre y apellidos:

Correo electrónico: