UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

Propuesta TFG. Curso 2025/2026

GRADO: Grado en Física

CÓDIGO DEL TFG: 267-226-2025/2026

1. DATOS BÁSICOS DEL TFG:

Título: Criptografía postcuántica: estado actual y revisión de algoritmos

Descripción general (resumen y metodología):

La criptografía postcuántica (PQC del inglés Post-Quantum Cryptography), también llamada "Criptografía resistente a la computación cuántica", se refiere a algoritmos criptográficos resistentes a ataques efectuados mediante computación cuántica.[]?

A este tipo de criptografía no pertenecen los algoritmos de clave pública más populares, que pueden ser superados por un ordenador cuántico suficientemente potente haciendo uso del algoritmo de Shor.[]?

Aunque los actuales ordenadores cuánticos experimentales no son aún capaces de atacar cualquier algoritmo criptográfico real, ya se están desarrollando algoritmos resistentes a esta amenaza.[]?

En el TFG propuesta se realizará un estudio bibliográfico sobre el impacto que tendrá la computación cuántica sobre los sistemas criptográficos actualmente utilizados, y la revisión de propuestas de algoritmos que tratan de dar respuesta a la futura amenaza que permitirá romper los cifrados actuales.

Tipología: Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

Objetivos planteados:

1. Características de los computadores cuánticos
2. Impacto del uso de la computación cuántica sobre los modelos de criptografía actuales
3. Estudio del algoritmo de Shor
4. La computación postcuántica
5. Revisión y comparativa de algoritmos criptográficos postcuánticos

Bibliografía básica:

- Estado de la criptografía post-cuántica y simulaciones de algoritmos post-cuánticos. Álvaro Rodrigo Reyes Rosado. Universidad Autónoma de Barcelona. Septiembre de 2018
- Desenmarañando el enredo cuántico de la ciberseguridad: ordenadores cuánticos, criptografía cuántica y post-cuántica. Gonzalo Álvarez Marañón. blogthinkbig.com. 20 de abril de 2021
- "New qubit control bodes well for future of quantum computing". phys.org.
- "Q&A With Post-Quantum Computing Cryptography Researcher Jintai Ding".
- Prueba cuántica de próxima generación PKI y certificados digitales. Giannis Naziridis . ssl.com. 16 de septiembre de 2021
- PQC Standardization Process: Third Round Candidate Announcement . Computer Security Resource Center. NIST 22 de julio de 2020
- POST-QUANTUM CRYPTOGRAPHY. Current state and quantum mitigation. v2. ENISA. Mayo de 2021

Recomendaciones y orientaciones para el estudiante:

Plazas: 1

2. DATOS DEL TUTOR/A:

Nombre y apellidos: JOSÉ LUIS BERNIER VILLAMOR

Ámbito de conocimiento/Departamento: ARQUITECTURA Y TECNOLOGÍA DE COMPUTADORES

Correo electrónico: jbernier@ugr.es

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

Nombre y apellidos:

Ámbito de conocimiento/Departamento:

Correo electrónico:

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:

Centro de convenio Externo:

5. DATOS DEL ESTUDIANTE:

Nombre y apellidos: Julia Díaz Canón

Correo electrónico: juliadc@correo.ugr.es