


Irakaslegoak aurkeztutako GRADU AMAIERAKO LANAREN proposamena	
Propuesta de TRABAJO FIN DE GRADO por parte del profesorado	BILBOKO INGENIARITZA ESKOLA ESCUELA DE INGENIERÍA DE BILBAO

GEHIENEZKO LUZERA: ORRI BAT (2 ALDEAK) / LONGITUD MÁXIMA 1 HOJA (2 CARAS)

DATU OROKORRAK / DATOS GENERALES

Lanaren izenburua / Título del trabajo: Evaluación de la criptografía cuántica frente a la clásica

Tutorea (gehienez bi) / Tutor-a (máx. 2): Mikel Egaña/ Iker Sobrón

e-mail: mikel.egana@ehu.eus / iker.sobron@ehu.eus

Hizkuntza / Idioma:  EUSKERA  CASTELLANO

Izena emateko aurrebaldintzak / Requisitos para apuntarse:
Sistemas de Gestión de Seguridad de Sistemas de Información (SGSSI)

DESKRIBAPEN ZEHASTUTA / DESCRIPCION DETALLADA

En este TFG se pretende investigar el estado del arte de algoritmos criptográficos post-quánticos como QKD (Quantum Key Distribution), implementarlo a nivel de simulación, y realizar un benchmarking de dichas tecnologías con algoritmos criptográficos actuales y con los post-cuánticos.

La idea surge del interés de Ikerlan en explorar las tecnologías cuánticas para la criptografía. La criptografía tiene un papel fundamental hoy en día. Protege nuestra información cuando viaja a través de Internet (data on-transit) y también cuando se almacena (at rest). La aparición de la computación cuántica con alto potencial de computación hace peligrar la seguridad de las soluciones criptográficas actuales y abre una nueva área de estudio en algoritmos criptográficos post-quantum. Hay artículos publicados sobre esta temática y existen trabajos de simulación de sistemas con diferentes problemáticas.

Este trabajo se realizará en Ikerlan (<https://www.ikerlan.es/>), en sus oficinas de Bilbao.

GrAL-AREN HELBURUAK / OBJETIVOS DEL TFG

- Realizar un estado del arte de técnicas de criptografía post-quantum.
- Realizar un estudio comparativo entre soluciones clásicas y cuánticas sobre criptografía basado en el estado del arte.

GrAL-AREN EKARPENAK / CONTRIBUCIONES DEL TFG

Conocer el desempeño de cada tecnología y el grado de vulnerabilidad de cada método.

ERABILIKO DIREN TRESNAK / HERRAMIENTAS A USAR

- Qiskit
- Python