GI2QKD. Gipuzkoa Quantum QKD, comunicaciones cuánticas ultraseguras

Consorcio: Ibermatica; i3B; Tecnalia

Tecnología: Quantum Computing

Descripción general:

En este proyecto se investiga en determinadas áreas de QKD y conexas, relacionadas con la protección de información, para acercar esta tecnología a las necesidades del mercado.

Los objetivos específicos son:

- OE1: Análisis de vulnerabilidad de los sistemas QKD disponibles.
- OE2: Estudio del rendimiento de los algoritmos QKD como BB84 y sus variantes.
- OE3: Investigación para la integración de las claves QKD en un sistema seguro clásico (IPSec, OpenTLS), como base de nuevos protocolos Post-cuánticos locales (PQC).
- OE4: Estudio e investigación en dinámicas de actualización y gestión de claves QKD.
- OE5: Experimentación sobre una configuración real de QKD, tanto a nivel físico, como a nivel de experimentación sobre sistemas de clústeres cuánticos distribuidos en la nube.
- OE6: Investigación para la adaptación de protocolos en Casos de Uso / servicios y evaluación del rendimiento del impacto de la capa QKD sobre servicios de bajo, medio y alto nivel (capa de trasporte, redes, voz ip, comunicaciones, túneles VPN, visión, etc.).

Programa: PROGRAMA GIPUZKOA QUANTUM

Duración: 12 meses (2023-2024)

Presupuesto global proyecto: 220.651,76 €

Presupuesto Grupo Ayesa: 220.651,76 €

Este proyecto ha sido objeto de ayuda con cargo al programa Red guipuzcoana de Ciencia, Tecnología e Innovación 2018 de Diputación de Gipuzkoa.

Gipuzkoako Foru Aldundia
Ekonomia Sustapeneko, Turismoko eta Landa Inguruneko Departamentua

Diputación Foral de Gipuzkoa
Departamento de Promoción Económica, Turismo y Medio Rural

GI2QKD. Gipuzkoa Quantum QKD, comunicaciones cuánticas ultraseguras

Consorcio: Ibermatica; i3B; Tecnalia

Tecnología: Quantum Computing

Rol de Ayesa:

Ibermática actúa como líder del proyecto GI2QKD, encargándose de la coordinación técnica, administrativa y económica del consorcio, así como de la gestión de riesgos, la supervisión del cumplimiento de hitos y la interlocución con las entidades financiadoras. Además, impulsa las actividades de difusión y transferencia de resultados mediante acciones de comunicación, generación de material divulgativo y contacto con los agentes interesados en las tecnologías de comunicaciones cuánticas seguras.

A lo largo del proyecto participa en la investigación sobre sistemas de distribución cuántica de claves (QKD), colaborando en el análisis del estado del arte, el estudio de vulnerabilidades y el modelado de arquitecturas de comunicación ultrasegura orientadas a su integración con servicios VPN y entornos clásicos de ciberseguridad. Su trabajo se centra especialmente en comprender cómo integrar tecnologías QKD dentro de infraestructuras reales y analizar sus posibles riesgos, limitaciones y vectores de ataque.

También contribuye al estudio de nuevas alternativas de integración entre sistemas clásicos y cuánticos, evaluando la incorporación de protocolos post-cuánticos (PQC), mecanismos híbridos de cifrado y soluciones de comunicación segura adaptadas a servicios empresariales. En este ámbito, participa en la comparación entre sistemas QKD físicos y virtuales, analizando costes, rendimiento y viabilidad operativa para escenarios reales de despliegue.

Dentro de la investigación experimental, IBERMÁTICA lidera las pruebas y simulaciones sobre entornos híbridos clásico-cuánticos, validando en laboratorio la integración de tecnologías QKD tanto en infraestructuras físicas como en sistemas virtualizados y distribuidos en la nube

Estas actividades permiten evaluar la aplicabilidad real de las soluciones investigadas y definir hojas de ruta para su futura implantación industrial.

Finalmente, desarrolla la capa de integración y explotación de servicios, creando frameworks y servicios API/REST que permiten conectar plataformas clásicas con simuladores y entornos cuánticos. Además, valida los resultados obtenidos desde el punto de vista de negocio y ciberseguridad, definiendo casos de uso, evaluando la escalabilidad de las soluciones y analizando su potencial aplicación en empresas interesadas en comunicaciones ultraseguras y criptografía post-cuántica.

.