UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
ESCUELA DE POSGRADO

MAESTRÍA EN CIENCIAS MENCIÓN INFORMÁTICA

TESIS

DISEÑO DE UN MODELO CUÁNTICO PARA MULTIPLICAR DATOS CIFRADOS PARA PRESERVAR SEGURIDAD

PARA OPTAR AL GRADO ACADÉMICO DE MAESTRO EN CIENCIAS MENCIÓN INFORMÁTICA

AUTOR
Br. KARLA CATHERINE ROJAS PEDRAZA

ASESOR:
Dr. LAURO ENCISO RODAS

CÓDIGO ORCID:
0000-0001-6266-0838

CUSCO –PERÚ
2026

Universidad Nacional de San Antonio Abad del Cusco

INFORME DE SIMILITUD

(Aprobado por Resolución Nro.CU-321-2025-UNSAAC)

El que suscribe, el **Asesor** LAURO ENCISO RODAS quien aplica el software de detección de similitud al trabajo de investigación/tesis titulada: DISEÑO DE UN MODELO CUÁNTICO PARA MULTIPLICAR DATOS CIFRADOS PARA PRESERVAR SEGURIDAD

Presentado por: KARLA CATHERINE ROJAS PEDRAZA DNI N° 41769537;
presentado por: ..... DNI N°: .....
Para optar el título Profesional/Grado Académico de MAESTRO EN CIENCIAS MENCIÓN INFORMÁTICA

Informo que el trabajo de investigación ha sido sometido a revisión por 2 veces, mediante el Software de Similitud, conforme al Art. 6° del ***Reglamento para Uso del Sistema Detección de Similitud en la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 1 **%.**

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No sobrepasa el porcentaje aceptado de similitud.	X
Del 11 al 30 %	Devolver al usuario para las subsanaciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, conforme al reglamento, quien a su vez eleva el informe al Vicerrectorado de Investigación para que tome las acciones correspondientes; Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de Asesor, firmo el presente informe en señal de conformidad y **adjunto** las primeras páginas del reporte del Sistema de Detección de Similitud.

Cusco, 06 de JULIO de 2026

Firma
Post firma Lauro Enciso Rodas
Nro. de DNI 23853228
ORCID del Asesor 0000-0001-6266-0838

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema de Detección de Similitud: **oid:** 27259:604621901

Karla Catherine Rojas Pedraza

DISEÑO DE UN MODELO CUÁNTICO PARA MULTIPLICAR DATOS CIFRADOS PARA PRESERVAR SEGURIDAD.pdf

Universidad Nacional San Antonio Abad del Cusco

Detalles del documento

Identificador de la entrega
trn:oid:::27259:604621901

Fecha de entrega
4 jul 2026, 6:51 a.m. GMT-5

Fecha de descarga
4 jul 2026, 7:53 a.m. GMT-5

Nombre del archivo
DISEÑO DE UN MODELO CUÁNTICO PARA MULTIPLICAR DATOS CIFRADOS PARA PRESERVAR SEG....pdf

Tamaño del archivo
1.6 MB

112 páginas

23.793 palabras

124.287 caracteres

1% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Coincidencias menores (menos de 15 palabras)

Fuentes principales

1% Fuentes de Internet
0% Publicaciones
1% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Caracteres reemplazados
45 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
ESCUELA DE POSGRADO

INFORME DE LEVANTAMIENTO DE OBSERVACIONES A TESIS

Dr. LEONCIO SOLIS QUISPE, Director de la Escuela de Posgrado, nos dirigimos a usted en condición de integrantes del jurado evaluador de la tesis intitulada **DISEÑO DE UN MODELO CUÁNTICO PARA MULTIPLICAR DATOS CIFRADOS PARA PRESERVAR SEGURIDAD** del / de la **Br. KARLA CATHERINE ROJAS PEDRAZA.** Hacemos de su conocimiento que el (la) sustentante ha cumplido con el levantamiento de las observaciones realizadas por el Jurado el día **VEINTICINCO DE JUNIO DE 2026**.

Es todo cuanto informamos a usted fin de que se prosiga con los trámites para el otorgamiento del grado académico de MAESTRO EN CIENCIAS MENCIÓN INFORMÁTICA.

Cusco, 03 de julio 2026

DR. JAVIER ARTURO ROZAS HUACHO
Primer Replicante

DR. JOSE LUIS SONCCO ALVAREZ.
Segundo Replicante

DR. HANS HARLEY CCACYAHUILLCA BEJAR
Primer Dictaminante

MTRO. IVAN CESAR MEDRANO VALENCIA
Segundo Dictaminante

Resumen

Esta tesis abordó el problema de la multiplicación segura de datos cifrados, donde se requiere preservar la seguridad y la integridad de los datos, con este objetivo se propuso el diseño y validación de un modelo híbrido – clásico cuántico – el cual multiplica polinomios cifrados, parte fundamental del criptosistema homomórfico aproximado Cheon–Kim–Kim-Song (CKKS), fundamentado en el problema Ring Learning With Errors (RLWE). Asimismo, esta solución empleó convoluciones cuánticas mediante la Quantum Fourier Transform (QFT), para explorar sus propiedades de interferencia y superposición en el dominio cuántico criptográfico. Metodológicamente, el modelo se implementó mediante circuitos cuánticos simulados utilizando el framework Qiskit, en conjunto con la librería criptográfica Microsoft SEAL y el lenguaje Python, lo que permitió evaluar el comportamiento del modelo en un entorno mixto – clásico cuántico. Los resultados obtenidos demostraron que el producto calculado sobre datos cifrados mediante un criptosistema homomórfico cuántico corresponde – dentro de un margen de error acotado y controlado – al producto en texto plano, validando que el uso de técnicas cuánticas en un criptosistema clásico no afecta la seguridad de los datos y preserva la fidelidad algebráica. Durante la multiplicación cuántica, los datos permanecieron ininteligibles, accesibles unicamente por un usuario autorizado, lo que constituye un aporte relevante y escalable para el desarrollo de modelos de procesamiento seguro de datos en escenarios cuánticos.

Palabras clave: Computación cuántica, Criptosistema homomórfico CKKS, Multiplicación cuántica, Seguridad de datos, Transformada Cuántica de Fourier

Abstract

This thesis addressed the challenge of secure multiplication over encrypted data, where information security and data integrity must be preserved. To this end, we proposed the design and validation of a hybrid classical-quantum model that multiplies encrypted polynomials, a foundational component of the Cheon–Kim–Kim-Song (CKKS) homomorphic encryption, grounded in the Ring Learning With Errors (RLWE). problem. Furthermore, the proposed solution leverages quantum convolutions by Quantum Fourier Transform (QFT), to explore quantum interference and superposition properties within the homomorphically encrypted domain. Methodologically, the model was implemented through simulated quantum circuits using the Qiskit framework, integrated with the Microsoft SEAL cryptographic library and the Python programming language. This approach enabled the evaluation of the model's performance within a hybrid classical–quantum environment. The results demonstrated that the product computed over homomorphically encrypted data corresponds–within a bounded and controlled error margin – to the plaintext product, thereby validating that the integration of quantum techniques into a classical cryptosystem does not compromise data security and preserves algebraic fidelity. Throughout the quantum multiplication process, the data remained unintelligible, accessible exclusively to authorized users. This constitutes a significant and scalable contribution to the development of secure data processing models within quantum environments.

Keywords: Quantum computing, CKKS homomorphic encryption, Quantum multiplication, Data security, Quantum Fourier Transform