

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

REIVINDICACIÓN DERIVADA DE TECNOLOGÍA

KFQUbit – Sistema Efímero de Cifrado Digital

Fecha: 04/11/2025

Titular: KFQUbit / Mauricio de Salvador

Expediente: Derivado de KFQU (Llave Fotónica Cuántica Universal)

Superintendencia de Industria y Comercio
adicionado: NC2025/0007410 Folios :2
dependencia:2020 Fecha:4/11/2025 3:32:32 p.
ipo aplicación: Complemento de información

1. TÍTULO DE LA INVENCION

Sistema efímero de cifrado digital implementado mediante llave cuántica fotónica universal (KFQUbit).

2. CAMPO DE LA INVENCION

La presente invención pertenece al campo de la criptografía avanzada y seguridad digital, particularmente a los sistemas de cifrado efímero, gestión de llaves de un solo uso y procesamiento seguro en memoria volátil (RAM). KFQUbit se constituye como una extensión tecnológica de la llave fotónica cuántica universal (KFQU), aplicada a entornos digitales donde el cifrado, descifrado y destrucción de llaves ocurren de manera inmediata y no persistente.

3. ANTECEDENTES DE LA INVENCION

Los sistemas tradicionales de cifrado almacenan parcial o temporalmente información sensible, llaves o metadatos, lo que los hace vulnerables a ataques forenses o intrusiones. La invención KFQU propuso originalmente una llave fotónica cuántica universal capaz de generar secuencias irrepetibles a partir de combinaciones fotónicas no deterministas. Sin embargo, la creciente demanda de seguridad digital en entornos empresariales, gubernamentales y militares exige implementaciones efímeras que garanticen que ninguna información permanezca tras su uso.

4. DESCRIPCIÓN TÉCNICA DE LA INVENCION (KFQUbit)

KFQUbit utiliza como núcleo la llave KFQU, la cual produce una secuencia cuántico-fotónica única denominada 'llave maestra efímera' que se traduce a una estructura digital encriptable. Esta llave es combinada con un token seguro generado mediante entropía mixta y un salt dinámico, conformando una doble capa de seguridad.

El sistema KFQUbit se compone de los siguientes módulos:

1. Módulo de cifrado efímero (MEF): ejecuta el cifrado en memoria RAM sin dejar rastros.
2. Módulo de generación de token seguro (MTS): crea una secuencia aleatoria de alta entropía compuesta por letras, números y símbolos.
3. Módulo de descifrado de un solo uso (MDU): permite la recuperación de información solo si se dispone del par llave-token correcto, autodestruyendo los datos tras su uso.
4. Módulo efímero RAM (MER): garantiza que toda la ejecución ocurre únicamente en memoria volátil, eliminando toda traza digital al finalizar la sesión.

5. REIVINDICACIONES

1. 1. Sistema de cifrado digital efímero basado en la llave cuántica fotónica universal (KFQU), caracterizado porque el proceso de cifrado y descifrado ocurre completamente en memoria volátil (RAM), destruyéndose automáticamente las llaves y tokens tras su uso.
2. 2. El sistema de la reivindicación 1, en el que cada sesión genera una única llave KFQubit, irrepetible y no reutilizable, vinculada a un token efímero alfanumérico-simbólico de alta entropía.
3. 3. El sistema de la reivindicación 1, en el que la llave KFQubit se autodestruye digitalmente tras finalizar el proceso de descifrado, volviendo inutilizable el archivo cifrado original.
4. 4. El sistema de la reivindicación 1, en el que no se almacenan metadatos ni información de usuario, garantizando cero retención de datos en el servidor o dispositivo intermedio.
5. 5. El sistema de la reivindicación 1, en el que el servidor actúa únicamente como canal de transporte temporal, sin capacidad de lectura ni registro de información cifrada.
6. 6. El sistema de la reivindicación 1, en el que el usuario puede operar la plataforma KFQubit mediante interfaz gráfica web o local, generando y gestionando sus llaves efímeras sin intervención de terceros.

6. RESUMEN (ABSTRACT)

La presente invención describe un sistema de cifrado digital efímero denominado KFQubit, derivado de la llave fotónica cuántica universal (KFQU). KFQubit permite cifrar y descifrar archivos de forma autónoma y autodestructiva, utilizando llaves únicas generadas en cada sesión y un token efímero de validación. Todo el proceso se ejecuta en memoria volátil, asegurando que ninguna llave, token o dato procesado quede almacenado en el servidor ni en el dispositivo del usuario. El sistema constituye una herramienta avanzada de seguridad digital orientada a entornos críticos civiles y gubernamentales.