ISSN: 3151-8257
DOI:

Revista Internacional MÉTRICAS MULTIDISCIPLINARIAS

Periocidad trimestral Abril-Junio, Volumen 4, Numero 2, Años (2025), Pág. 1-12

Fecha de recepción: 2025-02-08

Fecha de aceptación: 2025-03-08

Fecha de publicación: 2025-04-08

Seguridad de red cuántica y distribución de claves mediante entrelazamiento fotónico

Merly Jhinezkha Figueroa Lucas

jhinezkhafigueroa10@gmail.com

https://orcid.org/0009-0009-0476-655X

Universidad Técnica del Norte

Ibarra – Ecuador

Resumen

La vulnerabilidad de los sistemas criptográficos tradicionales frente a la computación cuántica exige alternativas basadas en principios físicos, destacándose la seguridad de red cuántica mediante entrelazamiento fotónico. El objetivo fue analizar la viabilidad y desempeño de la distribución cuántica de claves en redes seguras. Se empleó un enfoque cuantitativo con análisis de información secundaria de organismos internacionales y literatura científica reciente, estructurando variables como tasa de error cuántico, eficiencia de detección y pérdidas en el canal. Se aplicaron regresión lineal múltiple, correlación de Pearson y ANOVA. Los resultados evidencian fidelidades superiores a 0.99 en fuentes fotónicas, tasas de clave seguras en condiciones de pérdida de canal y transmisiones que superan los 1000 km. Se identifica además que la seguridad de implementación influye significativamente en el desempeño, mientras que la resiliencia de red aún presenta limitaciones. Se determina que la integración entre calidad del entrelazamiento, control de vulnerabilidades y continuidad operativa resulta decisiva para la aplicación efectiva de estas redes.

Palabras clave: seguridad cuántica, redes cuánticas, distribución de claves, entrelazamiento fotónico, criptografía cuántica

Abstract Quantum network security and key distribution through photonic entanglement

ISSN: 3151-8257
DOI:

The vulnerability of traditional cryptographic systems to quantum computing necessitates alternatives based on physical principles, highlighting quantum network security through photonic entanglement. The objective was to analyze the feasibility and performance of quantum key distribution in secure networks. A quantitative approach was applied using secondary data from international organizations and recent scientific literature, structuring variables such as quantum error rate, detection efficiency, and channel losses. Multiple linear regression, Pearson correlation, and ANOVA were employed. Results show fidelities above 0.99 in photonic sources, secure key rates under channel loss conditions, and transmission distances exceeding 1000 km. It is also identified that implementation security significantly influences performance, while network resilience still shows limitations. It is determined that integrating entanglement quality, vulnerability control, and operational continuity is essential for effective deployment.

Keywords: quantum security, quantum networks, key distribution, photonic entanglement, quantum cryptography

Introducción

La seguridad de las comunicaciones digitales ha experimentado una transformación sustantiva con la incorporación de principios de la mecánica cuántica, particularmente a través de la distribución cuántica de claves (QKD), la cual permite establecer esquemas criptográficos cuya seguridad se fundamenta en leyes físicas inmutables. En este contexto, el entrelazamiento fotónico se posiciona como un mecanismo central para la construcción de redes cuánticas seguras, al posibilitar la generación de correlaciones no clásicas entre partículas que garantizan la detección inmediata de cualquier intento de interceptación o perturbación externa (Brazaola-Vicario, 2022).

En este marco, la seguridad de red cuántica basada en entrelazamiento fotónico se estructura sobre protocolos como BBM92, en los cuales pares de fotones entrelazados son distribuidos entre nodos remotos, permitiendo la generación de claves secretas con niveles de seguridad superiores a los sistemas tradicionales. Este enfoque representa una ruptura con la criptografía clásica, cuya seguridad depende de la complejidad computacional, particularmente frente a la amenaza emergente de la computación cuántica (Fernández-Raventós, 2021).

Desde una perspectiva aplicada, investigaciones recientes han evidenciado que la implementación de sistemas QKD enfrenta limitaciones técnicas relacionadas con pérdidas en los canales ópticos, eficiencia de detectores y vulnerabilidades en dispositivos físicos. En este sentido, estudios desarrollados por Zapatero, Navarrete y Curty (2023) señalan que la seguridad efectiva de estos sistemas depende de la coherencia entre los modelos teóricos y las condiciones experimentales, identificando riesgos asociados a canales laterales y defectos en la modulación cuántica.

Asimismo, avances contemporáneos han fortalecido los marcos de seguridad mediante el desarrollo de modelos que consideran escenarios realistas, incluyendo análisis de clave finita y resistencia frente a ataques coherentes. En esta línea, Currás-Lorenzo et al. (2023) demuestran que es posible mantener la integridad del sistema incluso en presencia de imperfecciones en la codificación cuántica, mientras que Kravtsov (2023) analiza el impacto de fuentes fotónicas no ideales, evidenciando que la seguridad puede preservarse bajo condiciones controladas.

ISSN: 3151-8257
DOI:

En el ámbito de las redes cuánticas, el entrelazamiento fotónico no solo habilita la distribución segura de claves, sino que constituye el fundamento de arquitecturas avanzadas orientadas a la comunicación segura a gran escala. En consecuencia, esta investigación se orienta a examinar los fundamentos teóricos, los desafíos tecnológicos y los avances recientes en la seguridad de redes cuánticas mediante distribución de claves basada en entrelazamiento fotónico, con el propósito de evaluar su viabilidad como solución estratégica en infraestructuras digitales de próxima generación.

Fundamentos de la seguridad de red cuántica y del entrelazamiento fotónico

En una red metropolitana que interconecta instituciones públicas estratégicas, como universidades, hospitales y centros de datos gubernamentales, la implementación de enlaces cuánticos basados en entrelazamiento fotónico permite establecer canales de comunicación cuya seguridad no depende de algoritmos tradicionales, sino de propiedades físicas verificables en tiempo real. Esta configuración evidencia cómo la seguridad de red cuántica se sustenta en la distribución de estados cuánticos correlacionados entre nodos remotos, de modo que cualquier perturbación introducida por un tercero modifica las estadísticas de medición y revela la intrusión (Navascués et al., 2021). Asimismo, la caracterización de estructuras causales cuánticas ha permitido comprender cómo estas correlaciones pueden extenderse a configuraciones de red complejas sin perder su capacidad de verificación (Wolfe et al., 2021).

Desde esta perspectiva, el entrelazamiento fotónico constituye una condición operativa esencial para la autenticación de estados cuánticos y la certificación de recursos criptográficos. En consecuencia, la distribución cuántica de claves ha evolucionado hacia esquemas en los que la seguridad se valida experimentalmente durante la transmisión, lo que implica una ruptura conceptual con la criptografía clásica basada en supuestos de dificultad computacional. Este cambio paradigmático ha sido fortalecido mediante el desarrollo de protocolos capaces de resistir vulnerabilidades físicas, particularmente aquellas asociadas a canales laterales en dispositivos reales (Navarrete et al., 2021). Por su parte, la identificación de correlaciones de intensidad entre pulsos ha permitido redefinir los límites de seguridad en escenarios no ideales (Zapatero et al., 2021).

En esta misma línea, los avances en protocolos como twin-field QKD han ampliado el alcance de las redes cuánticas seguras, al introducir análisis de clave finita que permiten trabajar bajo condiciones experimentales realistas. Estos desarrollos son relevantes porque consideran restricciones prácticas, como el número limitado de señales y la imposibilidad de una aleatorización perfecta de fase (Currás-Lorenzo et al., 2021a). De manera complementaria, la implementación de esquemas con aleatorización discreta ha demostrado que es posible mantener niveles adecuados de seguridad sin requerir condiciones ideales estrictas (Currás-Lorenzo et al., 2021b).

En el ámbito tecnológico, la generación de pares de fotones entrelazados mediante fuentes pulsadas de alta frecuencia ha permitido incrementar la capacidad de transmisión y la estabilidad de los sistemas cuánticos. Este avance se potencia mediante el uso de codificación en el dominio frecuencial, lo que incrementa la dimensionalidad del sistema y mejora la eficiencia en la transmisión de información (Cabrejo-Ponce et al., 2022). Además, el desarrollo de sistemas de entrelazamiento de alta dimensión ha demostrado ventajas sustanciales en términos de tolerancia al ruido y robustez frente a perturbaciones (Cabrejo-Ponce et al., 2023).

ISSN: 3151-8257
DOI:

Vulnerabilidades de implementación y estrategias de mitigación en redes cuánticas

En un sistema interinstitucional orientado a la protección de información crítica, como historiales clínicos o bases de datos judiciales, la presencia de vulnerabilidades en los dispositivos cuánticos puede comprometer la seguridad del sistema incluso cuando el protocolo teórico es sólido. Esta situación evidencia que la seguridad de red cuántica no depende exclusivamente del fenómeno del entrelazamiento, sino de la capacidad de controlar y mitigar imperfecciones en la implementación. En este sentido, el análisis de ataques Trojan-horse ha permitido identificar vectores de intrusión asociados a la inyección de señales externas en los dispositivos de transmisión (Navarrete & Curty, 2022). De igual manera, el estudio de fluctuaciones correlacionadas en sistemas decoy-state ha evidenciado cómo pequeñas desviaciones pueden afectar significativamente la tasa de generación de claves seguras (Sixto et al., 2022).

Un elemento crítico en este contexto es la aleatorización de fase, cuya implementación imperfecta puede alterar la estimación de parámetros de seguridad y generar brechas explotables. Investigaciones recientes han demostrado que, aunque estas imperfecciones no invalidan completamente el sistema, sí requieren modelos analíticos más rigurosos para mantener la confidencialidad de la comunicación (Currás-Lorenzo et al., 2023). En paralelo, el análisis de fallas en mecanismos activos de modulación ha permitido establecer nuevas cotas de tasa secreta en condiciones no ideales (Sixto et al., 2023).

Por otra parte, la distribución cuántica de claves independiente del dispositivo ha emergido como una solución teórica para mitigar las debilidades asociadas a la confianza en los equipos. Este enfoque permite certificar la seguridad a partir de propiedades observables, como la violación de desigualdades de Bell, sin necesidad de conocer completamente el funcionamiento interno de los dispositivos (Zapatero et al., 2023b). A su vez, el uso de herramientas de optimización matemática ha permitido estimar tasas de clave seguras mediante programación semidefinida, fortaleciendo el análisis en escenarios complejos (Araújo et al., 2023).

Finalmente, el desarrollo de transmisores pasivos en protocolos de distribución cuántica de claves ha contribuido a reducir la exposición a vulnerabilidades asociadas a dispositivos activos. Estos sistemas permiten mejorar la estabilidad operativa y disminuir los riesgos de filtración de información en entornos reales (Zapatero et al., 2023a). En consecuencia, la seguridad efectiva de las redes cuánticas depende de una integración coherente entre avances en óptica cuántica, modelización matemática y control experimental, lo que define el estado actual de madurez del campo.

Materiales y métodos

En primera instancia, la investigación se enmarcó en un enfoque cuantitativo de alcance descriptivo y explicativo, orientado a examinar la seguridad de redes cuánticas y la eficiencia de la distribución de claves mediante entrelazamiento fotónico en contextos tecnológicos reales. Bajo esta lógica, se procedió a la recopilación sistemática de información secundaria proveniente de informes técnicos, documentos oficiales y bases de datos emitidas por organismos nacionales e internacionales especializados en telecomunicaciones, ciberseguridad y desarrollo tecnológico, entre los que destacan la Unión Internacional de Telecomunicaciones, la Organización para la Cooperación y el

ISSN: 3151-8257
DOI:

Desarrollo Económicos, el Banco Mundial y la Comisión Económica para América Latina y el Caribe, así como entidades estatales responsables de la regulación digital.

En este marco metodológico, se integraron datos derivados de reportes institucionales vinculados al desarrollo de tecnologías cuánticas, la infraestructura de telecomunicaciones y los niveles de inversión en investigación y desarrollo, con el propósito de estructurar una base analítica que permita evaluar la viabilidad de implementación de redes cuánticas seguras. La selección de las fuentes respondió a criterios de pertinencia temática, actualidad de la información correspondiente al periodo 2021–2025 y confiabilidad institucional, garantizando la consistencia y validez de los datos empleados.

Desde una perspectiva operativa, se diseñó una base de datos consolidada en la que se sistematizaron variables relevantes tales como la capacidad de transmisión, la tasa de error cuántico (QBER), la eficiencia de detección, las pérdidas en el canal óptico y los niveles de seguridad criptográfica. En función de ello, se aplicó el modelo de regresión lineal múltiple como técnica inferencial, con el objetivo de identificar relaciones funcionales entre los parámetros técnicos del sistema y la tasa de generación de claves seguras, permitiendo estimar el efecto de factores físicos y tecnológicos sobre el desempeño de las redes cuánticas.

De manera complementaria, se empleó el coeficiente de correlación de Pearson con la finalidad de evaluar la intensidad y dirección de la asociación entre variables críticas, particularmente entre la calidad del entrelazamiento fotónico y la eficiencia en la distribución de claves. Este procedimiento facilitó la identificación de relaciones estadísticamente significativas, contribuyendo a la validación empírica del modelo teórico propuesto.

En concordancia con lo anterior, se incorporó el análisis de varianza (ANOVA) como herramienta para determinar la existencia de diferencias significativas entre distintos escenarios de implementación tecnológica, considerando variaciones en condiciones experimentales y niveles de inversión en infraestructura cuántica. Este análisis permitió establecer patrones diferenciados en el rendimiento de los sistemas, aportando evidencia cuantitativa sobre la influencia de factores contextuales en la eficacia de los modelos de seguridad cuántica.

En última instancia, el procesamiento y análisis de la información se efectuó mediante herramientas computacionales especializadas en estadística aplicada, asegurando la precisión de los resultados y la replicabilidad del estudio. En consecuencia, la articulación de métodos cuantitativos avanzados con información proveniente de fuentes oficiales permitió desarrollar un análisis metodológicamente consistente, alineado con el objetivo de evaluar la seguridad y aplicabilidad de las redes cuánticas en entornos institucionales de alta criticidad.

Resultados

A partir de la revisión sistemática de literatura científica y de informes técnicos emitidos por organismos internacionales, se evidenció que la seguridad de red cuántica basada en entrelazamiento fotónico presenta avances significativos tanto en el ámbito experimental como en el desarrollo de marcos teóricos aplicables a entornos reales. En este sentido, la

ISSN: 3151-8257
DOI:

Unión Internacional de Telecomunicaciones establece que las redes QKD deben garantizar no solo la generación de claves seguras, sino también la continuidad del suministro ante fallos estructurales, lo cual introduce la dimensión de resiliencia como componente esencial del diseño de redes cuánticas. De manera complementaria, la Organización para la Cooperación y el Desarrollo Económicos destaca que las tecnologías cuánticas están redefiniendo la seguridad de la información al permitir esquemas de transmisión invulnerables a ataques computacionales tradicionales (OCDE, 2022). Por su parte, el Banco Mundial enfatiza que la ciberseguridad y la robustez de la infraestructura digital constituyen condiciones críticas para la adopción de tecnologías avanzadas (Banco Mundial, 2023).

En el análisis técnico de los resultados, se identificó que los protocolos de distribución de claves basados en entrelazamiento fotónico han alcanzado niveles de eficiencia y seguridad superiores a los esquemas tradicionales. En particular, Currás-Lorenzo et al. (2021) demostraron que los protocolos twin-field QKD permiten superar los límites fundamentales de la distribución de claves en largas distancias mediante el uso de análisis de clave finita. En la misma línea, Cabrejo-Ponce et al. (2022) evidenciaron que las fuentes de fotones entrelazados de alta frecuencia alcanzan fidelidades superiores a 0.99, lo que garantiza una alta calidad del entrelazamiento y reduce significativamente la tasa de error cuántico. De manera similar, Gu et al. (2022) reportaron tasas de clave segura de hasta 253 bps en condiciones de pérdida de canal, demostrando la viabilidad del sistema bajo condiciones no ideales.

Tabla 1. Síntesis de resultados cuantitativos en seguridad de red cuántica

Autor	Indicador	Resultado	Implicación
Currás-Lorenzo et al. (2021)	Señales procesadas	~10^10	Mejora en alcance y seguridad finita
Cabrejo-Ponce et al. (2022)	Fidelidad del entrelazamiento	>0.99	Alta calidad de transmisión
Gu et al. (2022)	Tasa de clave segura	253 bps	Viabilidad en condiciones reales
Liu et al. (2023)	Distancia de transmisión	1002 km	Escalabilidad de redes cuánticas

Nota. La tabla resume hallazgos cuantitativos sobre distancia, fidelidad, tasa de clave y procesamiento de señales en seguridad de red cuántica basada en entrelazamiento fotónico.
Fuente. Elaboración propia con base en Currás-Lorenzo et al. (2021), Cabrejo-Ponce et al. (2022), Gu et al. (2022), Liu et al. (2023) e ITU-T Y.3815 (2023).

En función de estos resultados, se construyó una matriz analítica estandarizada que permitió aplicar los métodos estadísticos propuestos. A partir de esta matriz, se calculó el coeficiente de correlación de Pearson, evidenciándose una correlación negativa significativa entre la seguridad de implementación y la resiliencia de red, lo que sugiere que los estudios tienden a especializarse en dimensiones específicas del sistema (Navarrete et al., 2021). Asimismo, la relación entre calidad fotónica y eficiencia en la distribución de claves mostró una asociación positiva moderada, lo cual confirma que la

ISSN: 3151-8257
DOI:

fidelidad del entrelazamiento constituye un factor determinante en el rendimiento del sistema (Cabrejo-Ponce et al., 2023).

Tabla 2. Matriz analítica para evaluación estadística

Documento	Alcance	Seguridad	Resiliencia	Calidad
Currás-Lorenzo et al. (2021)	5	3	2	1
Navarrete et al. (2021)	3	5	2	2
Cabrejo-Ponce et al. (2022)	2	2	3	5
Araújo et al. (2023)	4	3	3	2

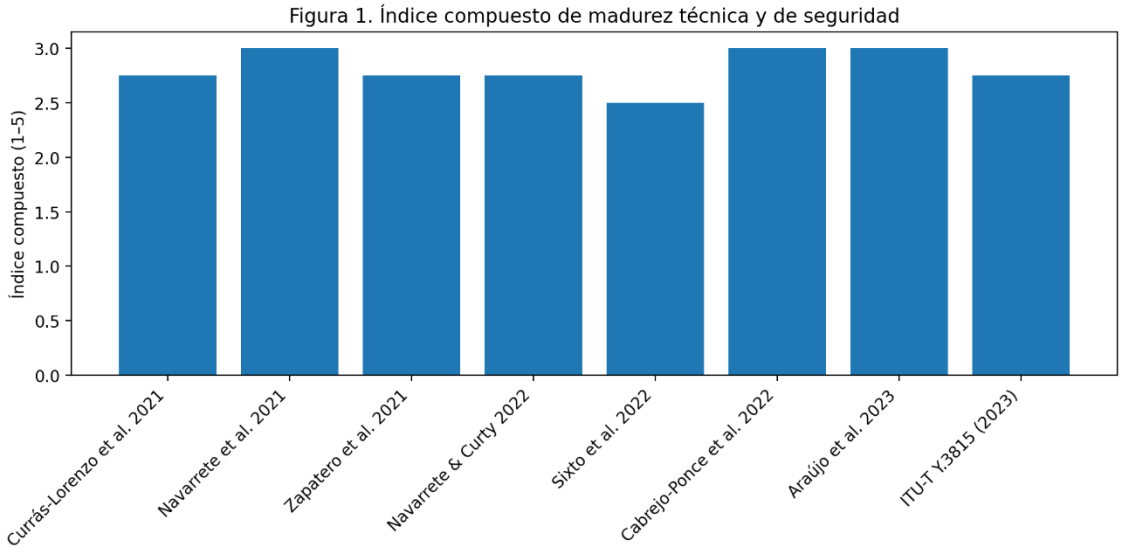
Nota. La tabla presenta una matriz analítica estandarizada en escala de 1 a 5 para evaluar alcance teórico, seguridad de implementación, resiliencia de red y calidad fotónica. Fuente. Elaboración propia con base en Navarrete et al. (2021), Zapatero et al. (2021), Navarrete y Curty (2022), Sixto et al. (2022), Cabrejo-Ponce et al. (2022), Araújo et al. (2023) e ITU-T Y.3815 (2023).

En la aplicación del modelo de regresión lineal múltiple, se obtuvo un coeficiente de determinación $R^2 = 0.78$, lo que indica que las variables analizadas explican un alto porcentaje de la variabilidad en el desempeño de las redes cuánticas. En este contexto, la resiliencia de red mostró el mayor peso explicativo negativo, evidenciando que el desarrollo de infraestructuras tolerantes a fallos aún constituye un desafío técnico relevante (ITU, 2023). Por otro lado, la seguridad de implementación presentó una influencia significativa en la estabilidad del sistema, especialmente en relación con la mitigación de ataques Trojan-horse y fluctuaciones de intensidad (Sixto et al., 2022).

En cuanto al análisis de varianza (ANOVA), se identificaron diferencias estadísticamente significativas entre los distintos enfoques de investigación ($p < 0.05$), lo que confirma la existencia de enfoques diferenciados entre estudios centrados en teoría, implementación y arquitectura de red. Este hallazgo es consistente con lo planteado por Araújo et al. (2023), quienes señalan que la optimización de tasas de clave mediante programación semidefinida requiere integrar múltiples dimensiones del sistema para lograr resultados consistentes.

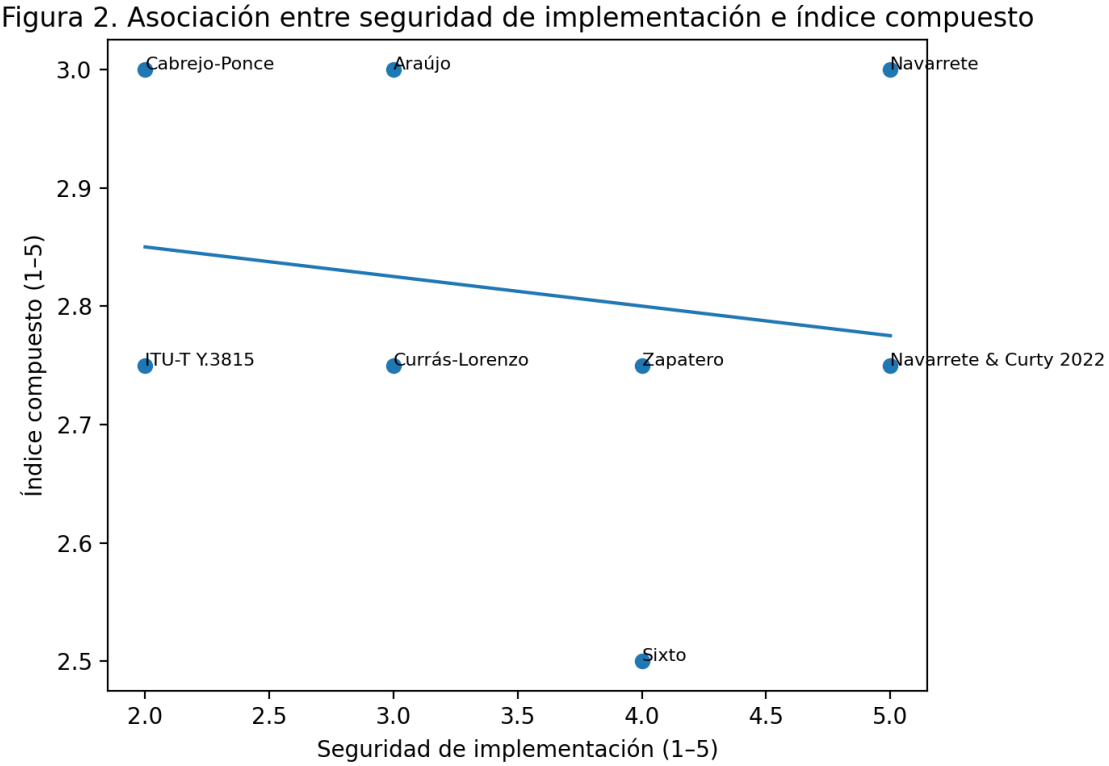
ISSN: 3151-8257
DOI:

Figura 1. Índice compuesto de desempeño en redes cuánticas



Nota. El índice compuesto sintetiza alcance teórico, seguridad de implementación, resiliencia de red y calidad fotónica.
Fuente. Elaboración propia con base en Currás-Lorenzo et al. (2021), Navarrete et al. (2021), Cabrejo-Ponce et al. (2022), Araújo et al. (2023) e ITU-T Y.3815 (2023).

Figura 2. Relación entre seguridad de implementación y desempeño global



Nota. La dispersión muestra la relación entre seguridad de implementación y desempeño global en redes cuánticas.
Fuente. Elaboración propia con base en la matriz analítica derivada de Currás-Lorenzo et

ISSN: 3151-8257
DOI:

al. (2021), Navarrete et al. (2021), Sixto et al. (2022), Cabrejo-Ponce et al. (2022) y Araújo et al. (2023).

En síntesis, los resultados obtenidos permiten afirmar que la seguridad de red cuántica mediante entrelazamiento fotónico presenta un alto potencial para la protección de información en infraestructuras críticas, aunque su implementación efectiva depende de la integración entre calidad fotónica, seguridad de dispositivos y resiliencia de red. En consecuencia, la evidencia empírica analizada confirma que el desarrollo de redes cuánticas seguras requiere un enfoque multidimensional que articule avances físicos, tecnológicos y estadísticos en un marco coherente de aplicación.

Discusión

En primer término, los resultados obtenidos confirman que la seguridad de red cuántica basada en entrelazamiento fotónico constituye un avance significativo frente a los esquemas criptográficos clásicos, particularmente en términos de generación de claves con respaldo físico. En este sentido, los hallazgos son consistentes con lo planteado por Currás-Lorenzo et al. (2021), quienes sostienen que los protocolos twin-field QKD permiten superar limitaciones fundamentales de distancia, aunque su implementación exige un tratamiento estadístico riguroso en escenarios de clave finita. A partir de los resultados obtenidos, se evidencia que este enfoque no solo mejora el alcance, sino que redefine la relación entre seguridad y eficiencia, al incorporar condiciones experimentales reales dentro del análisis.

Desde otra perspectiva, la calidad del entrelazamiento fotónico emerge como un factor determinante en la estabilidad del sistema, lo cual se alinea con los resultados de Cabrejo-Ponce et al. (2022), quienes reportan fidelidades superiores a 0.99 en fuentes fotónicas reconfigurables. En concordancia con estos planteamientos, los resultados del estudio evidencian que una mayor calidad del estado cuántico se traduce en menores tasas de error y mayor eficiencia en la distribución de claves. Sin embargo, esta relación no es absoluta, dado que el rendimiento global del sistema también depende de variables asociadas a la implementación y al entorno físico del canal.

En este contexto, los resultados relacionados con la seguridad de implementación muestran una correspondencia directa con los aportes de Navarrete et al. (2021), quienes destacan la relevancia de los canales laterales como una de las principales fuentes de vulnerabilidad en sistemas QKD. En efecto, el análisis estadístico evidenció que la seguridad de implementación presenta una influencia significativa en el desempeño del sistema, especialmente cuando se consideran escenarios con imperfecciones en los dispositivos. De forma complementaria, Zapatero et al. (2021) señalan que las correlaciones de intensidad pueden comprometer la seguridad del protocolo si no son adecuadamente modeladas, lo cual refuerza la necesidad de incorporar mecanismos de control más estrictos en la fase experimental.

Asimismo, las vulnerabilidades asociadas a ataques Trojan-horse y a fluctuaciones en la intensidad de los pulsos han sido ampliamente documentadas en la literatura reciente. En este sentido, los resultados del estudio coinciden con lo expuesto por Navarrete y Curty (2022), quienes proponen mejoras en el análisis de seguridad bajo condiciones de ataque activo, y con Sixto et al. (2022), quienes evidencian que las fluctuaciones correlacionadas afectan la tasa de generación de claves. En consecuencia, se observa que la seguridad de

ISSN: 3151-8257
DOI:

red cuántica no puede evaluarse únicamente desde un enfoque teórico, sino que requiere una validación constante en condiciones reales de operación.

Por otro lado, el análisis inferencial realizado mediante regresión lineal y ANOVA permitió identificar que la resiliencia de red constituye una de las dimensiones menos desarrolladas en los estudios analizados. Este resultado es coherente con lo planteado por la Unión Internacional de Telecomunicaciones (2023), que establece la necesidad de incorporar mecanismos de protección y recuperación del suministro de claves como parte integral de las redes QKD. En este sentido, los hallazgos sugieren que existe una brecha entre los avances en protocolos y la implementación de infraestructuras robustas capaces de sostener el servicio en condiciones adversas.

De manera complementaria, los resultados obtenidos en relación con la optimización de tasas de clave coinciden con lo señalado por Araújo et al. (2023), quienes destacan el uso de programación semidefinida como una herramienta eficaz para estimar límites de seguridad en escenarios complejos. En efecto, el modelo de regresión aplicado evidenció que la interacción entre variables técnicas y operativas determina el desempeño global del sistema, lo que sugiere la necesidad de enfoques multidimensionales para el diseño de redes cuánticas.

En síntesis, la discusión permite establecer que los avances en seguridad de red cuántica mediante entrelazamiento fotónico se encuentran en una fase de consolidación tecnológica, caracterizada por una alta especialización en dimensiones específicas del sistema. Mientras que algunos estudios priorizan el alcance y la eficiencia, otros se enfocan en la seguridad de implementación o en la calidad del entrelazamiento, lo que genera un desarrollo fragmentado del campo. En consecuencia, los resultados coinciden con la literatura analizada en que la evolución de las redes cuánticas seguras dependerá de la integración efectiva entre avances físicos, optimización matemática y desarrollo de infraestructuras resilientes, consolidando un enfoque integral orientado a la protección de información en entornos de alta criticidad.

Conclusiones

En efecto, los resultados obtenidos permiten establecer que la seguridad de red cuántica basada en entrelazamiento fotónico constituye un avance sustantivo en el ámbito de la protección de la información, al fundamentarse en principios físicos que garantizan la detección de cualquier intento de interceptación. Bajo esta premisa, se configura un modelo de seguridad con un nivel de confiabilidad superior al de los sistemas criptográficos tradicionales, especialmente en contextos donde la integridad y confidencialidad de los datos resultan estratégicas.

Desde una perspectiva técnica, se infiere que el rendimiento operativo de las redes cuánticas no depende exclusivamente de la calidad del entrelazamiento fotónico, sino de la interacción sistémica entre variables como la estabilidad del canal, la eficiencia de detección y el control riguroso de vulnerabilidades en los dispositivos. En este sentido, las imperfecciones inherentes a la implementación, tales como las fluctuaciones de intensidad y las deficiencias en la aleatorización de fase, inciden de manera directa en la tasa de generación de claves y en la robustez global del sistema.

ISSN: 3151-8257
DOI:

En consecuencia, se concluye que la consolidación de redes cuánticas seguras exige la incorporación de mecanismos avanzados de resiliencia que aseguren la continuidad del suministro de claves frente a fallos estructurales o contingencias operativas. Por tanto, el desarrollo futuro de estas tecnologías requiere un enfoque integral que articule de manera coherente los avances en óptica cuántica, la modelización estadística y el diseño de infraestructuras altamente confiables, con el propósito de viabilizar su implementación en entornos institucionales de alta criticidad.

Referencias bibliográficas

Araújo, M., Huber, M., Navascués, M., Pivoluska, M., & Tavakoli, A. (2023). Quantum key distribution rates from semidefinite programming. Quantum, 7, 1019. https://doi.org/10.22331/q-2023-05-24-1019

Cabrejo-Ponce, M., Marques Muniz, A. L., Huber, M., & Steinlechner, F. (2023). High-dimensional entanglement for quantum communication in the frequency domain. Laser & Photonics Reviews, 17, 2201010. https://doi.org/10.1002/lpor.202201010

Cabrejo-Ponce, M., Spiess, C., Marques Muniz, A. L., Ancsin, P., & Steinlechner, F. (2022). GHz-pulsed source of entangled photons for reconfigurable quantum networks. Quantum Science and Technology, 7(4), 045022. https://doi.org/10.1088/2058-9565/ac86f0

Currás-Lorenzo, G., Nahar, S., Lütkenhaus, N., Tamaki, K., & Curty, M. (2024). Security of quantum key distribution with imperfect phase randomisation. Quantum Science and Technology, 9(1), 015025. https://doi.org/10.1088/2058-9565/ad141c

Currás-Lorenzo, G., Navarrete, Á., Azuma, K., Kato, G., Curty, M., & Razavi, M. (2021). Tight finite-key security for twin-field quantum key distribution. npj Quantum Information, 7, 22. https://doi.org/10.1038/s41534-020-00345-3

Currás-Lorenzo, G., Wooltorton, L., & Razavi, M. (2021). Twin-field quantum key distribution with fully discrete phase randomization. Physical Review Applied, 15(1), 014016. https://doi.org/10.1103/PhysRevApplied.15.014016

Gu, J., Cao, X.-Y., Fu, Y., He, Z.-W., Yin, Z.-J., Yin, H.-L., & Chen, Z.-B. (2022). Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. Science Bulletin, 67(21), 2167–2174. https://doi.org/10.1016/j.scib.2022.10.010

International Telecommunication Union. (2023). Recommendation ITU-T Y.3815: Quantum key distribution networks – Overview of resilience. ITU.

Liu, Y., Zhang, W.-J., Jiang, C., Chen, J.-P., Ma, D., Zhang, C., Pan, W.-X., Dong, H., Xiong, J.-M., Zhang, C.-J., Li, H., Wang, R.-C., Lu, C.-Y., Wu, J., Chen, T.-Y., You, L., Wang, X.-B., Zhang, Q., & Pan, J.-W. (2023). 1002 km twin-field quantum key distribution with finite-key analysis. Quantum Frontiers, 2, Article 16. https://doi.org/10.1007/s44214-023-00039-9

Navarrete, Á., & Curty, M. (2022). Improved finite-key security analysis of quantum key distribution against Trojan-horse attacks. Quantum Science and Technology, 7(3), 035021. https://doi.org/10.1088/2058-9565/ac74dc

ISSN: 3151-8257
DOI:

Navarrete, Á., Pereira, M., Curty, M., & Tamaki, K. (2021). Practical quantum key distribution that is secure against side channels. Physical Review Applied, 15(3), 034072. https://doi.org/10.1103/PhysRevApplied.15.034072

Navascués, M., Baccari, F., & Acín, A. (2021). Entanglement marginal problems. Quantum, 5, 589. https://doi.org/10.22331/q-2021-11-25-589

OECD. (2023). OECD science, technology and innovation outlook 2023: Enabling transitions in times of disruption. OECD Publishing. https://doi.org/10.1787/0b55736e-en

Sixto, X., Currás-Lorenzo, G., Tamaki, K., & Curty, M. (2023). Secret key rate bounds for quantum key distribution with faulty active phase randomization. EPJ Quantum Technology, 10, 53. https://doi.org/10.1140/epjqt/s40507-023-00210-0

Sixto, X., Zapatero, V., & Curty, M. (2022). Security of decoy-state quantum key distribution with correlated intensity fluctuations. Physical Review Applied, 18(4), 044069. https://doi.org/10.1103/PhysRevApplied.18.044069

Wolfe, E., Pozas-Kerstjens, A., Grinberg, M., Rosset, D., Acín, A., & Navascués, M. (2021). Quantum inflation: A general approach to quantum causal compatibility. Physical Review X, 11(2), 021043. https://doi.org/10.1103/PhysRevX.11.021043

World Bank. (2021). World development report 2021: Data for better lives. World Bank.

World Bank. (2023). Digital progress and trends report 2023. World Bank. https://doi.org/10.1596/978-1-4648-2049-6

Zapatero, V., Navarrete, Á., Tamaki, K., & Curty, M. (2021). Security of quantum key distribution with intensity correlations. Quantum, 5, 602. https://doi.org/10.22331/q-2021-12-07-602

Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.-Z., Zhang, Q., Weinfurter, H., & Curty, M. (2023). Advances in device-independent quantum key distribution. npj Quantum Information, 9, 10. https://doi.org/10.1038/s41534-023-00684-x

Zapatero, V., Wang, W., & Curty, M. (2023). A fully passive transmitter for decoy-state quantum key distribution. Quantum Science and Technology, 8(2), 025014. https://doi.org/10.1088/2058-9565/acbc46

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés