


Pipeline para la validación de protocolos de comunicación post-cuántica basados en TF-QKD

Sergio Vázquez-Pozo¹  and Juan Manuel Murillo² 

¹ Universidad de Extremadura, Cáceres, España
svazquezzp@gmail.com

² Universidad de Extremadura, Cáceres, España
juanmamu@unex.es

Resumen Los protocolos actuales de comunicación post-cuántica permiten establecer comunicaciones seguras en distancias del orden de 15 kilómetros. Al intentar extender este alcance hasta distancias reales (1000 a 12000 km), el rendimiento del canal se ve significativamente degradado debido a turbulencias atmosféricas y otros fenómenos físicos que introducen ruido en la transmisión. En este contexto, los protocolos basados en Twin-Field Quantum Key Distribution (TF-QKD) han surgido como una estrategia prometedora para aumentar el rango de las comunicaciones cuánticas seguras. Sin embargo, la validación experimental de estos protocolos requiere despliegues a gran escala, cuyos costes económicos y logísticos resultan inasumibles. Para abordar este problema, este artículo presenta un pipeline de simulación y validación agnóstico al protocolo que permite evaluar la viabilidad de protocolos de comunicación post-cuántica sin necesidad de realizar despliegues reales. El enfoque propuesto integra métricas del estado del canal en el análisis de seguridad, proporcionando un entorno controlado, auditable y económicamente viable para analizar su comportamiento antes de acometer costosos experimentos físicos.

Keywords: TF-QKD · Arquitectura de Software · Simuladores · Seguridad Componible

1. Introducción

Desde la propuesta fundacional del protocolo BB84 [1], la comunicación cuántica persigue maximizar la tasa de generación de clave manteniendo una garantía de seguridad. Sin embargo, los enlaces directos convencionales están físicamente restringidos por el límite PLOB (Pirandola-Laurenza-Ottaviani-Banchi) [2], el cual dicta que la tasa de generación de clave decae exponencialmente con la distancia debido a la pérdida de fotones. Para superar esta barrera, la distribución cuántica de claves de campo gemelo (Twin-Field Quantum Key Distribution, TF-QKD) ha emergido como una arquitectura prometedora, permitiendo mayores distancias sin requerir repetidores cuánticos [4].

A pesar de este avance teórico, la transición de TF-QKD hacia un despliegue real vía satélite presenta desafíos de ingeniería. Recientes hitos experimentales



han logrado demostrar TF-QKD en espacio libre simulando el grosor atmosférico [7] a distancias de 14,2 km. No obstante, para enlazar continentes en los rangos habituales (1000 a 12000 km), la señal cuántica debe atravesar la atmósfera sufriendo aberraciones de fase y atenuación debido a la turbulencia.

A nivel experimental, operar bajo este nivel de ruido obliga a aplicar heurísticas de software que descarten las ventanas temporales donde la señal se vuelve irre recuperable. El reto radica en que cualquier protocolo moderno debe garantizar la *seguridad componible* [6]. Este paradigma asegura formalmente que la probabilidad de fallo total del sistema está estrictamente acotada por una métrica $\varepsilon_{\text{total}} = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}$ (donde ε_{sec} es el error de confidencialidad y ε_{cor} el de corrección). Cumplir con esta propiedad garantiza que la clave generada es matemáticamente indistinguible de una clave ideal. Sin embargo, demostrar empíricamente esta propiedad desplegando infraestructura aeroespacial tiene un coste económico demasiado alto, haciendo imperativa su validación previa en entornos de simulación. El propósito de este trabajo en curso es presentar el diseño de un *pipeline* de orquestación, adaptable a diversos protocolos cuánticos, que integra de forma nativa el filtrado físico del canal con la demostración criptográfica formal. Esta arquitectura proporciona el entorno auditable necesario para certificar la viabilidad teórica de los enlaces intercontinentales antes de acometer su costosa implementación física.

A continuación, se analizan los antecedentes (Sección 2), se detalla el diseño y el funcionamiento del *pipeline* propuesto (Sección 3), y se exponen las conclusiones derivadas (Sección 4).

2. Antecedentes

Tradicionalmente, el desarrollo de las redes de comunicación cuánticas ha estado supeditado a validaciones físicas en laboratorio o a través de enlaces de corta distancia. No obstante, escalar estas experimentaciones a escenarios satelitales choca con una barrera económica. Desplegar infraestructura aeroespacial únicamente para probar la viabilidad de un protocolo frente a la turbulencia atmosférica resulta inmensamente caro. Por consiguiente, la industria demanda poder certificar la robustez de cualquier algoritmo mediante simulaciones previas a su construcción.

Sin embargo, las metodologías de validación por software actuales revelan deficiencias arquitectónicas operando en silos aislados: se simula el comportamiento del canal; a continuación, se aplican rutinas de preprocesamiento *ad-hoc* para descartar el ruido de manera opaca y finalmente, se inyecta el remanente de datos procesados en los algoritmos de prueba de seguridad. Esta metodología elude validar con rigor el comportamiento del sistema bajo estrés. Postergando estas pruebas al momento del despliegue con condiciones físicas y ambientales reales.

Esta omisión es incompatible con los estándares de la seguridad componible, sustentados en teoremas criptográficos como el de Acumulación de Entropía Generalizado (GEAT) [5]. El GEAT parte de la premisa del peor caso: cualquier

alta varianza o porción de datos descartada se atribuye inmediatamente a la interferencia de un ciberatacante. Al carecer de un conducto formal de software que certifique ante el teorema que dicha varianza se debió legítimamente a fluctuaciones ambientales, el sistema matemático aplica una penalización extrema en la simulación, provocando que la tasa de comunicación colapse.

Surge, por tanto, la necesidad de trascender el diseño de protocolos específicos y desarrollar un procedimiento universal de validación de protocolos que no eluda tener en consideración las pruebas de estrés. Se requiere un procedimiento que pueda acoplarse a cualquier algoritmo cuántico, integrando la telemetría ambiental con la validación matemática. El beneficio obtenido sería el de poder demostrar con garantías la viabilidad teórica de las redes intercontinentales antes de afrontar su costosa implementación. A continuación mostramos nuestra propuesta para este procedimiento de validación.

3. Pipeline de Simulación

Proponemos un pipeline de validación estructurado en tres capas (Figura 1) para vincular la simulación física con la validación criptográfica. El diseño es agnóstico y adaptable a diversos protocolos cuánticos. Su núcleo consiste en extraer métricas del canal y empaquetarlas como metadatos estructurados, facilitando el cálculo de la seguridad componible sin degradar el rendimiento de la red.

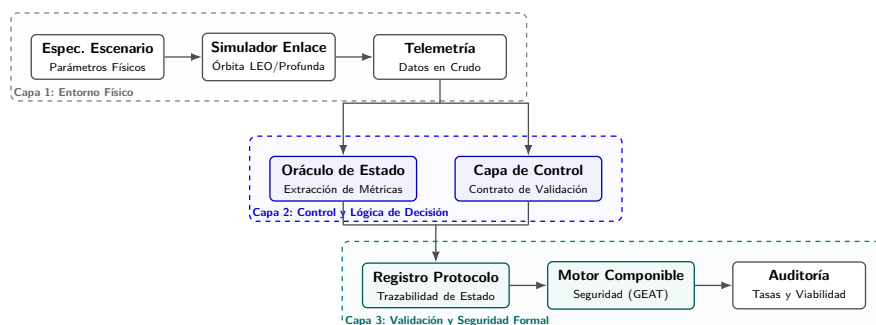


Figura 1. Desglose funcional de la arquitectura.

El flujo opera secuencialmente, garantizando la trazabilidad del dato. En primer lugar, la Capa 1 (entorno físico) simula la dinámica del canal a partir de los parámetros de la infraestructura, emitiendo telemetría ruidosa. A continuación, la Capa 2 (control) procesa esta información mediante un oráculo de estado encargado de extraer una métrica de salud del canal. A modo de ejemplo, este oráculo puede evaluar la topología de la red para asignar una etiqueta discreta, como “Entorno Hostil” o “Estable”, contrastando el resultado empírico contra umbrales de aceptación.

Finalmente, en la Capa 3 (seguridad formal), los paquetes validados se almacenan junto a su etiqueta de estado en un registro inmutable. Al inyectar estos datos enriquecidos en un motor criptográfico como el GEAT, el algoritmo incorpora el contexto ambiental en su cálculo. Esta trazabilidad estructural evita que la atenuación natural de la atmósfera se asuma erróneamente como la intervención activa de un adversario, mitigando así penalizaciones sobre la tasa de clave y garantizando la seguridad componible.

Esta arquitectura mitiga el riesgo financiero inherente a los despliegues satelitales. Al desvincular la simulación física de la validación formal, cualquier protocolo puede someterse a pruebas de estrés. Si el canal incumple los criterios de control, el motor rechaza las garantías criptográficas. Esta metodología auditable permite iterar el diseño del protocolo y asegurar su viabilidad teórica antes de asumir los elevados costes de implementación física.

4. Conclusiones

A través de este trabajo, argumentamos que escalar las comunicaciones post-cuánticas a distancias intercontinentales (1000–12000 km) no es únicamente un desafío físico, sino un problema abierto de Arquitectura de Software. Las metodologías tradicionales basadas en flujos de ejecución *ad-hoc* penalizan matemáticamente los sistemas en entornos ruidosos. Nuestra propuesta ilustra cómo la integración sistemática de telemetría y teoría de seguridad componible mediante oráculos de estado puede sortear estas penalizaciones de forma segura. Como trabajo futuro, la investigación se centrará en estandarizar el Registro de Protocolo (Capa 3) para facilitar su integración nativa en diferentes entornos de trabajo, consolidando así su aplicabilidad industrial.

Referencias

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, 175–179 (1984).
2. Pirandola, S., Laurenza, R., Ottaviani, C., Banchi, L.: Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017). doi:10.1038/ncomms15043
3. Liao, S.-K. *et al.*: Satellite-to-ground quantum key distribution. *Nature* **549**, 43–47 (2017). doi:10.1038/nature23655
4. Lucamarini, M., *et al.*: Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018). doi:10.1038/s41586-018-0066-6
5. Metger, T., Renner, R.: Security of quantum key distribution from generalised entropy accumulation. *Nat. Commun.* **14**, 5272 (2023). doi:10.1038/s41467-023-40920-8
6. Portmann, C., Renner, R.: Security in quantum cryptography. *Rev. Mod. Phys.* **94**, 025008 (2022). doi:10.1103/RevModPhys.94.025008
7. Li, Y., Zeng, T., *et al.*: Free-Space Twin-Field Quantum Key Distribution. *arXiv preprint arXiv:2503.17744* (2025). doi:10.48550/arXiv.2503.17744

