

MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2026-2027

PROPUESTA

Título:	<i>Desarrollo e implementación en FPGA de técnicas de procesamiento digital de señal (DSP) para sistemas de distribución cuántica de claves de variable continua (CV-QKD)</i>
Título en inglés:	<i>Development and FPGA Implementation of Digital Signal Processing (DSP) Techniques for Continuous-Variable Quantum Key Distribution (CV-QKD) Systems</i>
Tutor/es:	<i>Adrián Llanos Velasco, Andrés Ruiz Chamorro</i>
Correos-e:	<i>adrian.llanos@qddynamics.es, andres.ruiz@qddynamics.es</i>
Lugar de realización:	<i>Tres Cantos, Madrid</i>

Resumen:

La distribución cuántica de claves de variable continua (CV-QKD, Continuous-Variable Quantum Key Distribution) permite establecer claves criptográficas seguras codificando la información en las cuadraturas del campo electromagnético de estados coherentes de luz, que se miden mediante detección coherente (homodina o heterodina) con un oscilador local. A diferencia de los sistemas de variable discreta, la CV-QKD utiliza componentes estándar de las comunicaciones ópticas coherentes —láseres de telecomunicación, moduladores IQ, fotodiodos balanceados y convertidores analógico-digitales de alta velocidad—, lo que la hace especialmente atractiva para su integración en las redes de fibra actuales.

El precio de esta compatibilidad es que casi toda la complejidad del sistema se traslada al procesamiento digital de señal (DSP): la recuperación de portadora y de fase a partir de tonos piloto, la sincronización de reloj y de trama, la compensación de desbalance IQ y de la respuesta del receptor, el filtrado adaptado, el submuestreo y la estimación de parámetros como la varianza del ruido de disparo o el ruido en exceso. En los sistemas actuales gran parte de esta cadena de DSP se ejecuta fuera de línea en un ordenador, lo que limita la tasa de clave alcanzable y dificulta el funcionamiento continuo del enlace. Migrar estas etapas a hardware reconfigurable (FPGA) es el paso necesario para disponer de sistemas CV-QKD compactos, en tiempo real y desplegables comercialmente.

El objetivo de este Trabajo de Fin de Máster es diseñar, implementar y validar en FPGA una o varias de las etapas de la cadena de DSP de un receptor CV-QKD, partiendo de la implementación de referencia existente en software (Python) y llegando a una implementación en tiempo real que procese las muestras de los ADC del sistema. El trabajo se realizará sobre el sistema CV-QKD experimental disponible en el centro de realización (Tres Cantos, Madrid), y se evaluará en términos de exactitud respecto a la referencia en software, latencia, rendimiento (throughput), consumo de recursos de la FPGA y, en última instancia, tasa de clave secreta obtenida.

Metodología:

El trabajo se desarrollará en las siguientes fases:

- **Revisión bibliográfica:** estudio de la arquitectura de un sistema CV-QKD con oscilador local en el receptor (protocolo de modulación gaussiana, tonos piloto,

detección coherente) y de las técnicas de DSP que emplea, con especial atención a las que ya se utilizan en receptores ópticos coherentes clásicos.

- **Modelo de referencia en software:** estudio y caracterización de la cadena de DSP de referencia, implementada en Python, verificándola con trazas reales capturadas del sistema experimental. Servirá como referencia funcional y como fuente de vectores de prueba para el hardware.
- **Particionado y diseño de la arquitectura:** análisis de la cadena de DSP para seleccionar las etapas que se implementarán en la FPGA, y definición de la arquitectura hardware y del formato numérico más adecuados para cada una de ellas.
- **Implementación en FPGA:** descripción del hardware en VHDL/Verilog o mediante síntesis de alto nivel (HLS), simulación funcional con los vectores de prueba del modelo de referencia, y síntesis e implementación sobre las FPGA de Xilinx (AMD) disponibles en el laboratorio, con análisis de tiempos y de ocupación de recursos.
- **Integración y validación experimental:** integración de los bloques en el sistema de adquisición del receptor CV-QKD, comparación bit a bit o estadística de los resultados con la referencia en software y medida del impacto sobre el ruido en exceso y la tasa de clave secreta del enlace.
- **Documentación:** redacción de la memoria con la descripción de la arquitectura, los resultados obtenidos y las posibles líneas de continuación (integración de etapas adicionales, optimización de recursos, procesado en tiempo real de extremo a extremo).

Las herramientas previstas son Python para el modelo de referencia, el entorno de diseño de Xilinx (Vivado y Vitis HLS), simuladores HDL y el instrumental óptico y electrónico del laboratorio.

Conocimientos previos recomendados:

Es suficiente con una base sólida de electrónica digital y de procesado de señal. En concreto, se recomienda:

- Procesado digital de señal: muestreo, filtrado digital (FIR/IIR), transformada de Fourier, aritmética en coma fija y efectos de cuantificación.
- Diseño digital y FPGA: lenguajes de descripción de hardware (VHDL o Verilog), flujo de diseño con herramientas comerciales, simulación y análisis de tiempos. Se valorará la experiencia con síntesis de alto nivel (HLS) y con plataformas SoC.
- Fundamentos de comunicaciones ópticas y detección coherente (modulación IQ, oscilador local, recuperación de portadora).
- Programación en Python para el modelado y la verificación.
- Nivel de inglés suficiente para la lectura de artículos científicos y documentación técnica.

Bibliografía:

- [1] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015. doi: 10.3390/e17096072.
- [2] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—The theory of practical implementations," *Adv. Quantum Technol.*, vol. 1, 1800011, 2018. doi: 10.1002/qute.201800011.

- [3] Y. Zhang, Y. Bian, Z. Li, S. Yu and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Appl. Phys. Rev.*, vol. 11, 011318, 2024. doi: 10.1063/5.0179566.
- [4] F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev and H. Hübel, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," *Quantum*, vol. 3, 193, 2019. doi: 10.22331/q-2019-10-07-193.
- [5] H.-M. Chin, N. Jain, D. Zibar, U. L. Andersen and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," *npj Quantum Inf.*, vol. 7, 20, 2021. doi: 10.1038/s41534-021-00361-x.
- [6] N. Jain et al., "Practical continuous-variable quantum key distribution with composable security," *Nat. Commun.*, vol. 13, 4740, 2022. doi: 10.1038/s41467-022-32161-y.
- [7] A. Ruiz-Chamorro, D. Cano, A. Garcia-Callejo and V. Fernandez, "Effects of experimental impairments on the security of continuous-variable quantum key distribution," *Heliyon*, vol. 9, no. 6, e16670, 2023. doi: 10.1016/j.heliyon.2023.e16670.
- [8] A. Ruiz-Chamorro, A. Garcia-Callejo and V. Fernandez, "Low-complexity continuous-variable quantum key distribution with true local oscillator using pilot-assisted frequency locking," *Sci. Rep.*, vol. 14, 10770, 2024. doi: 10.1038/s41598-024-61461-0.
- [9] S. Sarmiento, J. Tabares and S. Etcheverry, "Low-complexity CV-QKD system with optical pilot-tone local oscillator synchronization," *arXiv preprint arXiv:2509.12735*, 2025.
- [10] D. Solar Nikolic, "Secure real-time transmitter for continuous variable quantum key distribution," Ph.D. thesis, Department of Physics, Technical University of Denmark, 2019.
- [11] S. J. Savory, "Digital coherent optical receivers: Algorithms and subsystems," *IEEE J. Sel. Top. Quantum Electron.*, vol. 16, no. 5, pp. 1164–1179, 2010. doi: 10.1109/JSTQE.2010.2044751.
- [12] E. Ip, A. P. T. Lau, D. J. F. Barros and J. M. Kahn, "Coherent detection in optical fiber systems," *Opt. Express*, vol. 16, no. 2, pp. 753–791, 2008. doi: 10.1364/OE.16.000753.
- [13] J. G. Proakis and D. G. Manolakis, *Digital Signal Processing: Principles, Algorithms, and Applications*, 4th ed. Pearson, 2007.
- [14] U. Meyer-Baese, *Digital Signal Processing with Field Programmable Gate Arrays*, 4th ed. Springer, 2014.
- [15] S. Kilts, *Advanced FPGA Design: Architecture, Implementation, and Optimization*. Wiley-IEEE Press, 2007.