**Resumen**

Las redes de telecomunicaciones de nueva generación, como 5G e IoT, requieren nuevas medidas de seguridad que impliquen el manejo y control de la información, equilibrando la seguridad y el uso eficiente de los recursos computacionales. El uso de la misma arquitectura de computación (CPU) para la ejecución de procesos de algoritmos criptográficos, como el cifrado simétrico AES-128 y la función hash SHA-256, provoca el sobrecalentamiento de la CPU, lo que limita el uso de la red para otras aplicaciones. Se describe el diseño, implementación y verificación de aceleradores de hardware en SoC-FPGA, utilizando bibliotecas de AMD Vitis y HLS. La arquitectura diseñada se encarga de migrar de forma automática el trabajo computacional que se realiza en el Componente de Procesamiento hacia la Lógica Programable y el trabajo de control de gestión de datos en el sistema operativo Linux embebido mediante el uso de AXI de alto rendimiento y controladores de flujo. El diseño también contempla la verificación de la funcionalidad usando vectores de prueba de NIST y la comparación de la latencia y el uso de recursos lógicos. De acuerdo con los resultados experimentales, el sistema presenta un rendimiento de 59.5 MB/s para el algoritmo de cifrado AES-128 y 12.6 MB/s utilizando el algoritmo SHA-256. Aunque la frecuencia de operación de la FPGA es menor que la de un microprocesador de escritorio, la arquitectura dedicada libera la carga de trabajo del microprocesador y brinda un comportamiento estable y determinístico al procesar grandes cantidades de datos. Por lo anterior, la diversidad de arquitecturas de soporte es factible para la implementación de nodos de edge computing donde la disponibilidad del sistema y la eficiencia en el uso de la energía es lo más importante.

*Palabras clave:* SoC-FPGA, aceleración en hardware, criptografía, Vitis Libraries, síntesis de alto nivel High-Level Synthesis.

**Abstract**

Establishing new security techniques for protection mechanisms on telecommunications systems such as 5G and IoT must be strategically planned to determine how information can be best protected while optimizing the value of available computing resources. Typical encryption and hashing blanket implementations on processors such as AES-128 and SHA-256, create a saturation of the central processing unit and can cause network application bandwidth to be lost. The present degree assignment explains the design, implementation, and evaluation of the hardware accelerators on the Zynq-7000 SoC-FPGA, using the AMD Vitis and High Level Synthesis (HLS) bibliographic method. The created architecture transfers processing-intensive activities from the Processing System (PS) to the Programmable Logic (PL) and performs data transfers using high throughput AXI interfaces under the control of an Embedded Linux Operating System. The method addresses the functional verification of the design using NIST test vectors and latency, and logic (LUT and DSP) resources) utilization comparative analysis. It has been shown that the designed system achieves a throughput of 59.5 MB/s and 12.6 MB/s for AES-128 and SHA-256, respectively. Although the operating frequency of the FPGA is lower than that of a desktop CPU, the developed architecture can relieve the system's main processor and provide steady and predictable performance when handling large blocks of data. The design is suitable for edge computing nodes, as it meets design flexibility and power efficiency constraints.

*Keywords:* SoC-FPGA, Hardware acceleration, Cryptography, Vitis Libraries, High-Level Synthesis.