Investigación de Cores IP modulares postcuánticos para comunicación segura mediante túneles criptográficos "on-demand". Cores-Brigde-PQC

1. Objetivos

El objetivo principal del proyecto Cores-Brigde-PQC es el diseño y desarrollo de una familia de Cores IP criptográficos postcuánticos para ser implementados sobre FPGA y/o como parte del diseño inicial de ASICs, mediante RTL en lenguaje VHDL.

Los Cores IP se diferenciarán en dos grandes grupos: núcleos criptográficos y núcleos de pila TCP/IP. Los núcleos criptográficos realizarán operaciones de criptografía postcuántica, ML-KEM y ML-DSA y criptografía de clave simétrica, AES-256, mientras que los núcleos TCP/IP permitirán operar y modificar protocolos de red.

El proyecto combinará estos núcleos en un diseño capaz de utilizar dos o más FPGAs para establecer túneles criptográficos postcuánticos, transparentes y gestionados por los propios Cores IP, con el fin de facilitar conexiones seguras a través de internet entre ordenadores u otros periféricos conectados.

Los objetivos específicos incluyen el diseño de criptocores postcuánticos y clásicos, el diseño del stack TCP/IP para integración en redes, la investigación de funciones no clonables físicamente PUF, junto con generadores de números aleatorios TRNG, la validación del dispositivo en entorno controlado y el desarrollo de un script de configuración basado en un paradigma de confianza cero.

2. En qué consiste el proyecto

Cores-Brigde-PQC consiste en el desarrollo de un conjunto de Cores IP que actuarán como componente de infraestructura de red para establecer un túnel seguro basado en criptografía postcuántica entre ordenadores u otros elementos de red, a través de internet y sin requerir una configuración específica o una modificación sustancial de la infraestructura IT.

Tras la implementación del proyecto, los resultados esperados se centrarán, por un lado, en obtener una serie de Cores IP dedicados a dos grandes tareas: criptografía postcuántica y clásica y gestión de protocolos de internet; y, por otro lado, en disponer de un script capaz de configurar dos o más dispositivos FPGA de bajo coste para el establecimiento de un túnel postcuántico no invasivo para el resto de la organización.

El dispositivo físico constará, en su mínima expresión, de un chip FPGA, dos puertos Ethernet y un lector de tarjetas SD. Inicialmente, los dispositivos estarán sin configurar. Para configurarlos, existirá un script de compilación que utilizará el código fuente para crear una configuración única e irrepetible para el túnel que se pretende crear.

La parte más sensible de la configuración serán los certificados y claves privadas necesarios para la autenticación de los dispositivos. Al finalizar el proceso de compilación, las claves quedarán guardadas como parte del hardware, dentro del bitstream, es decir, el archivo de configuración final de la FPGA. Tras la obtención del bitstream, los productos intermedios de la compilación podrán eliminarse para reducir la posibilidad de filtraciones de información sensible.

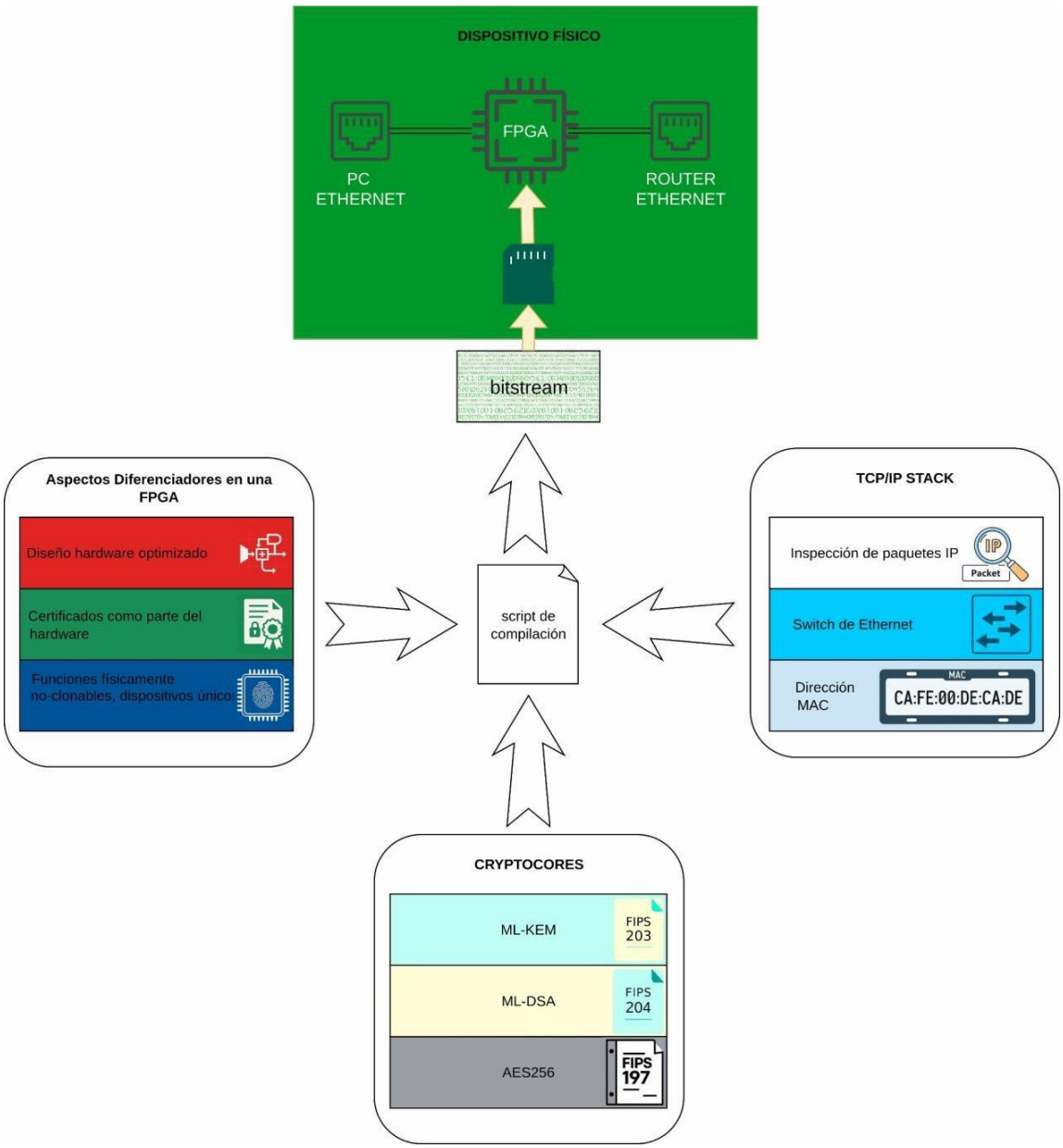

Figura 1. Componentes principales del diseño

El diseño contendrá los Cores IP criptográficos ML-KEM, ML-DSA y AES-256, así como los Cores IP que permitirán a la FPGA establecerse como elemento de red. Estos Cores podrán utilizarse de forma conjunta en el dispositivo propuesto o independientemente por terceros. Todos los elementos estarán orquestados por el script de compilación, que producirá los certificados y la configuración necesaria de forma local, facilitando un paradigma de confianza cero.

Una vez configuradas, las FPGAs podrán desplegarse en los entornos correspondientes, como servidores corporativos, usuarios o sistemas que se quieran integrar en el túnel. La característica fundamental del túnel es que no captura la totalidad del tráfico como una VPN,

sino únicamente el tráfico dirigido a una o varias direcciones IP preseleccionadas. El resto de la red queda intacta, salvo por una configuración mínima en el router que gestiona el servidor.

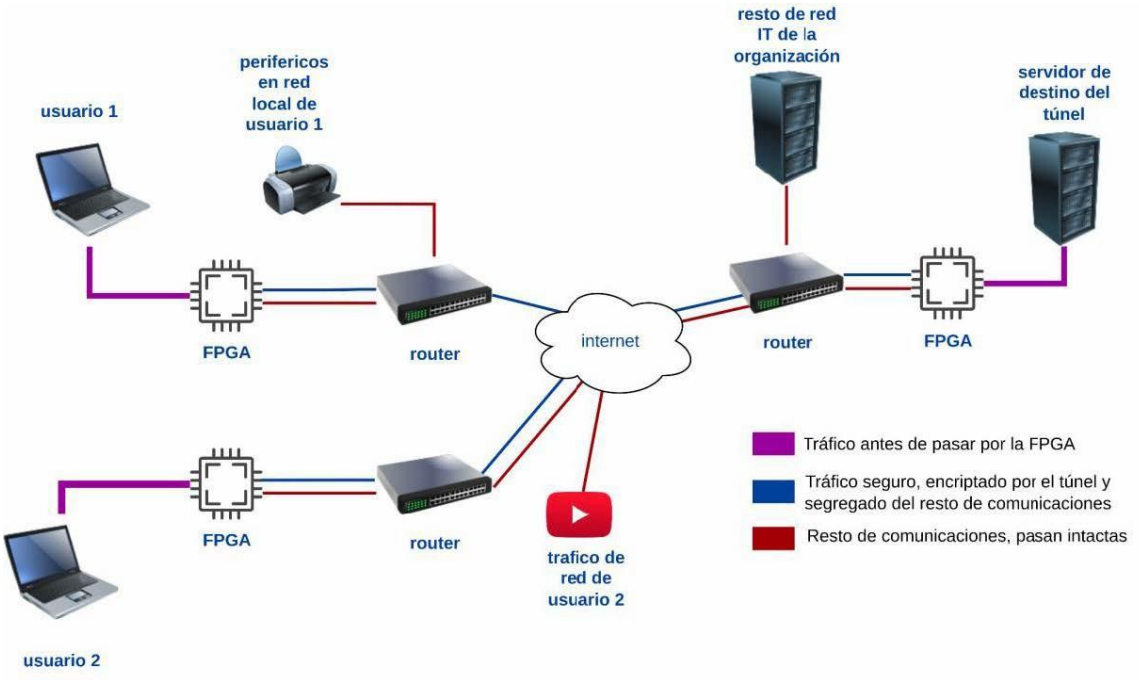

Figura 2. Esquema típico de conexión

Con esta estrategia, la FPGA inspecciona el tráfico entrante y saliente. Cuando la IP de los paquetes coincide con las direcciones preconfiguradas, los paquetes se cifran o descifran mediante el túnel. Cuando no coinciden, se dejan pasar intactos. De este modo, se obtiene un túnel criptográfico transparente que permite reforzar comunicaciones concretas sin alterar el funcionamiento general de la infraestructura IT

3. Aplicaciones / usos

El ámbito de aplicación de los Cores IP desarrollados será principalmente la ciberseguridad, especialmente en comunicaciones punto a punto que requieran protección frente a amenazas derivadas de la computación cuántica.

La aplicación principal del proyecto será la creación de un túnel criptográfico plug-and-play, capaz de integrarse en una infraestructura IT existente sin alterarla. Este túnel permitirá cifrar el flujo de datos seleccionado mediante FPGA, mientras que el resto del tráfico continuará funcionando sin modificaciones.

La propuesta también podrá aplicarse a entornos donde sea necesario reforzar comunicaciones entre sistemas conectados, servidores, ordenadores u otros periféricos, especialmente cuando se busque una transición hacia criptografía postcuántica sin cambiar el sistema completo ni actualizar todos los elementos de red.

Además, al tratarse de Cores IP modulares desarrollados en RTL puro, los núcleos criptográficos y los núcleos TCP/IP podrán utilizarse conjuntamente en el dispositivo propuesto o por separado en diseños de terceros que necesiten funciones criptográficas, de red o una futura implementación sobre FPGA o ASIC.

Entre los resultados esperados destacan los Cores IP de criptografía híbrida de bajo coste, los Cores IP para stack TCP/IP, el túnel criptográfico plug-and-play, la generación de entropía resistente a ataques y el script de configuración con paradigma de confianza cero.

4. Estado del arte e innovación tecnológica

El estado del arte parte de la necesidad de reforzar los sistemas de comunicación actuales ante el avance de la computación cuántica. La criptografía clásica se basa en problemas matemáticos como la factorización de enteros, los logaritmos discretos o las curvas elípticas, que podrían verse comprometidos por algoritmos cuánticos como Shor y Grover.

En este contexto surge la criptografía postcuántica (PQC), orientada a desarrollar algoritmos seguros frente a ataques clásicos y cuánticos. El NIST ha liderado un proceso de selección y estandarización de algoritmos postcuánticos, entre los que se encuentran ML-KEM para intercambio de claves, ML-DSA para firma digital y SPHINCS+.

La transición hacia PQC no consiste únicamente en sustituir algoritmos, sino que implica adaptar protocolos, dispositivos de red, sistemas embebidos e infraestructuras digitales. Actualmente, muchas soluciones se orientan a actualizar software o modificar protocolos existentes, lo que puede suponer costes elevados y dificultades de implantación.

Frente a este enfoque, Cores-Brigde-PQC plantea una solución basada en hardware: introducir una FPGA entre el elemento de red y el router para crear un túnel criptográfico transparente. Esta aproximación permite añadir protección postcuántica sin modificar de forma sustancial la infraestructura IT existente.

La innovación principal del proyecto reside en combinar, en una misma solución, criptografía híbrida ML-KEM, ML-DSA y AES-256, stack TCP/IP, generación de entropía reforzada y configuración local mediante bitstream. Además, el uso de PUFs junto con una fuente externa de entropía permite generar semillas únicas por dispositivo, reforzando la seguridad del sistema.

Como novedad tecnológica, el proyecto propone un dispositivo basado en FPGA capaz de actuar como túnel criptográfico postcuántico, con Cores IP modulares, reutilizables, agnósticos al fabricante y con posibilidad de evolución futura hacia ASICs. Su finalidad es facilitar una transición hacia comunicaciones resistentes a la computación cuántica con el menor impacto posible sobre la infraestructura existente.