Perfil (FD) Codi projecte: PID2023-148649OB-I00

El projecte amb codi PID2023-148649OB-I00 (finançat per l'Agència Estatal d'Investigació) del Departament d`Enginyeria Electrònica (710) de la Universitat Politècnica de Catalunya (UPC) convoca la sol·licitud d'un doctorand en el projecte anomenat: Implementación de sistemas criptobiométricos post-cuánticos sobre RISC-V.

Descripció del lloc de Treball

Se ofrece un contrato de 4 años para la realización de una tesis doctoral en el departamento d'Enginyeria Electrònica de la Universitat Politècnica de Catalunya. La temática de la tesis doctoral se centrará en uno o varios de los objetivos propuestos en el proyecto de investigación, a saber:

- Integración de RISC-V sobre FPGA e interconexión de módulos hardware específicos.
- Desarrollo de aceleradores hardware para identificación biométrica compatibles con RISC-V.
- Diseño de aceleradores hardware para criptografía post-cuántica adaptables a RISC-V. Aplicación sobre los algoritmos de McEliece y Cristals-Kyber.
- Propuestas de integración conjunta de sistemas biométricos y criptográficos orientados a la protección de plantillas biométricas y generación de claves

Perfil candidat/a

Debido al carácter multidisciplinar del proyecto, el candidato/a debe poseer un Máster en Ingeniería, Ciencias computacionales (informática), Matemáticas o Física. Por otro lado, se valoran positivamente conocimientos en las siguientes temáticas:

- Capacidad de trabajo autónomo y en equipo.
- Lenguaje de programación hardware VHDL.
- Experiencia en la implementación de sistemas digitales sobre FPGAs.
- Conocimientos en lenguajes de programación de alto nivel tipo C, Phyton, etc.
- Dominio de Matlab y sistema operativo Linux.
- Conocimientos básicos en álgebra lineal y teoría de Galois.
- Se requiere de un alto nivel de inglés. El candidato deberá presentar los avances de su tesis doctoral en congresos internacionales, de modo que debe estar capacitado para expresarse, realizar escritos y presentaciones en esta lengua.

Breu descripció del projecte:

Los enormes avances que se han producido en el campo de la física y la fotónica, han sido cruciales para el advenimiento de los ordenadores cuánticos, cuya capacidad para resolver cierto tipo de algoritmos es muy superior a la que ofrecen los microprocesadores clásicos. La seguridad en las transacciones electrónicas, o la confidencialidad de la información que circula por canales no seguros, está actualmente garantizada por la robustez que ofrecen algoritmos criptográficos como RSA o ECC. Sin embargo, la comunidad científica es consciente de que en un futuro próximo la tecnología cuántica convertirá en obsoletos dichos algoritmos, y consecuentemente la seguridad de muchos sistemas se verá claramente amenazada. Conocedores de esta problemática, el NIST lanzó en 2017 una llamada donde interpelaba a la comunidad internacional a presentar algoritmos que fuesen resistentes a ataques post cuánticos y que pudieran devenir en los nuevos estándares criptográficos. En 2022, y tras final la tercera ronda de evaluación de los candidatos, Cristals-Kyber fue elegido como nuevo estándar, y se abrió la puerta a que otro algoritmo también pudiera convertirse en estándar criptográfico

.

De forma coetánea en el tiempo, otros investigadores, han trabajado intensamente en desarrollar microprocesadores libres de regalías que pudieran competir con ARM, el microprocesador que utiliza más del 70% de los dispositivos electrónicos que hay en el mercado. El resultado ha sido RISC-V, un microprocesador desarrollado inicialmente- por investigadores de la universidad de California-Berkeley, que ha despertado un gran interés entre la comunidad científica debido a las prestaciones que ofrece. Desde que se anunció que Cristals-Kyber se convertía en nuevo estándar criptográfico, ha habido varias publicaciones que proponían su implementación sobre RISC-V. Las propuestas que se han hecho tienen varios inconvenientes: son válidas únicamente para unos parámetros muy

concretos; los aceleradores que incluyen no son reprogramables; y suelen resolver funcionalidades de muy alto nivel, lo que los convierte en poco flexibles.
De forma paralela a estas dos líneas de investigación, hay una tercera que se orientaba a combinar algoritmos criptográficos post cuánticos con sistemas de identificación biométrica. El objetivo era doble: almacenar las plantillas biométricas y realizar autenticación de usuarios con seguridad post cuántica. En este sentido, lo habitual ha sido escoger algoritmos basados en corrección de errores, como Classic McEliece, dado que facilitaba la integración conjunta de ambos sistemas.

El proyecto CRIPTORISC tiene por objetivo realizar contribuciones en las tres líneas mencionadas, a saber:

a) Desarrollar aceleradores hardware para identificación biométrica compatibles con la arquitectura RISC-V.

b) Diseño de aceleradores hardware para criptografía post cuántica adaptables a RISC-V. Se pretenden diseñar dos aceleradores: uno orientado a criptografía basada en corrección de errores y otro para criptografía basada en retículos.

c) Explorar las posibilidades que ofrece CRISTALS-KYBER en el desarrollo de criptosistemas biométricos orientados a la protección de plantillas biométricas y generación de claves.