

# (QKD-Cascade) - QKD-Cascade

## Información de contacto

### Dirección: Investigadores principales:

- VICENTE MARTIN AYUSO

[vicente.martin@upm.es](mailto:vicente.martin@upm.es)

### Otros investigadores UPM:

- Jesús Martínez Mateo
- David Elkouss Coronas

## Tipo de oferta tecnológica

Software

## Áreas de investigación e innovación

- Tecnologías digitales, Inteligencia Artificial, ciberseguridad, 5G, robótica

## ¿Dónde?

Centro de Investigación en Simulación Computacional (CCS) Grupo de investigación en Información y Computación Cuántica (GIICC)

## Descripción del software

El presente programa, QKD-Cascade, implementa el protocolo Cascade utilizado en la capa de corrección de errores de los sistemas de distribución cuántica de claves (QKD en adelante). El protocolo, definido en "Secret-key reconciliation by public discussion" LNCS 765, permite corregir una cadena de bits intercambiada entre dos extremos de una comunicación. Esa cadena de bits es lo que conocemos como clave en un sistema QKD, y los extremos (o interlocutores) son referidos como Alice y Bob.

La característica principal del protocolo Cascade es que permite .corregir un porcentaje de error elevado (como es el caso en los sistemas QKD donde podemos encontrar probabilidades de error que pueden oscilar entre el 2% y el 8%), al mismo tiempo que intenta minimizar la cantidad de información (bits de paridad) proporcionada para realizar la corrección.

## Referencia

M-008489/2009