(QKD-Cascade) – QKD-Cascade

Contact information

Address: Main researchers:

- VICENTE MARTIN AYUSO

  vicente.martin@upm.es

Other UPM researchers:

- Jesús Martínez Mateo
- David Elkouss Coronas

Technological Offers type

Software

Research and innovation areas

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

Where?

Computer Simulation Research Centre Quantum Information and Computing Research Group (GIICC)

Software description

The QKD-Cascade program uses the Cascade protocol in the error correction layer on quantum key distribution (QKD) systems. The protocol, defined in Secret-key reconciliation by public discussion LNCS 765, allows a string of bits exchanged between two ends of a communication to be corrected. The bit string is what we know as key in a QKD system and the ends (or callers) are referred to as Alice and Bob.
The main feature of the Cascade protocol is enabling correction of a high error percentage (as is the case in QKD systems where we can come across error probabilities that may waive between 2% and 8%), while trying to minimise the amount of information (parity bits) provided to make the correction.

Reference

M-008489/2009