

OFERTA DE BECA DE INVESTIGACIÓN

EL GRUPO TENCALCRYPT DE LA UNIVERSIDAD DE ALCALÁ DE HENARES OFRECE:

BECA DE INTRODUCCIÓN A LA INVESTIGACIÓN

TÍTULO: Introducción a la criptografía postcuántica y Machine Learning aplicado al criptoanálisis

DURACIÓN: 5 MESES.

CUANTÍA: 750 EUROS/MES (BRUTOS).

PERFIL Y REQUISITOS: SE BUSCA ALUMNO DE MÁSTER O BIEN DE ÚLTIMO CURSO DE GRADO. SE VALORARÁ UNA BUENA BASE MATEMÁTICA, BUEN CONOCIMIENTO DE PYTHON Y/O C, ASÍ COMO INTERÉS EN LA CRIPTOGRAFÍA Y EN LA INVESTIGACIÓN.

DESCRIPCIÓN: El alumno aprenderá las principales ideas de la criptografía basada en retículos (RLWE), el enfoque más prometedor en criptografía postcuántica y el que más propuestas mantiene en el concurso NIST para su estandarización. El objetivo es estudiar una nueva propuesta de criptoanálisis basada en técnicas de Machine Learning (regresión multivariable y redes neuronales).

El becario trabajará con nosotros pero no es imprescindible que resida físicamente en la comunidad de Madrid.

La beca deberá solicitarse a través de la web de la Universidad. El proceso de solicitud se abrirá durante la próxima quincena en la sección de convocatorias de I+D+I/becas de investigación. No obstante, se puede dirigir correo (y así se recomienda) al profesor-tutor para aclaraciones informales.

CONTACTO: Iván Blanco-Chacón (ivan.blancoc@uah.es)