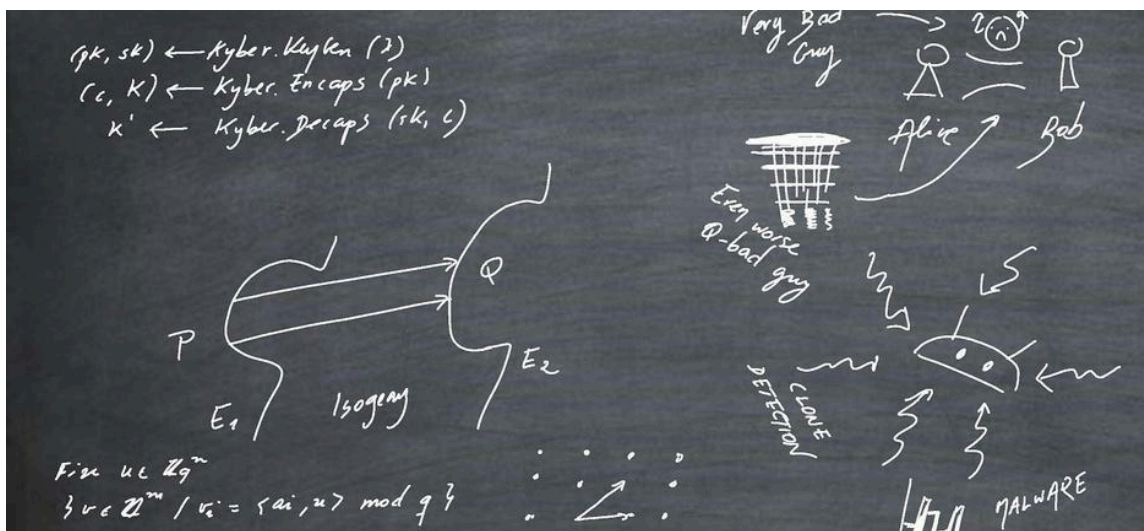




CryptoClub

SESIÓN INAUGURAL TERCERA EDICIÓN

Miércoles 14 de Octubre - Aula 1.A.01, Campus de Puerta de Toledo

15:00 Apertura

- **Bienvenida institucional:** Prof. D. César Huete de Lira, Director de la Escuela Politécnica Superior de la U. Carlos III de Madrid.
- **Intervención Subdirector Academia Ciberinteligencia del CNI**
- Intervención **coordinadores** de la iniciativa: **Prof. Juan M. Estevez Tapiador** y **Prof. María Isabel González Vasco**

15:30 Conferencia Inaugural: D. Eduardo Soria-Vázquez

Calcular en secreto: un paseo por la criptografía de la computación

Abstract: ¿Es posible calcular sobre datos que no podemos ver? ¿Y convencer a otros de que un programa se ha ejecutado correctamente sin que tengan que repetirlo? En las últimas décadas, la criptografía ha pasado de proteger únicamente la información en tránsito o en reposo a proteger también la información *mientras se usa*. Esta charla ofrece un recorrido introductorio y resultados recientes en tres de los grandes paradigmas de la criptografía de la computación: el cifrado completamente homomórfico (FHE), que permite operar directamente sobre datos cifrados; la computación verificable (VC), que permite comprobar de forma eficiente la corrección de un cálculo delegado y la computación segura multipartita (MPC), donde varias partes calculan conjuntamente una función sin revelar sus entradas privadas.

16:15 APERITIVO

