



Seminario Rubio de Francia

Conferencia

por

David Pérez García

Universidad Complutense de Madrid

Título:

Desigualdades de Sobolev en criptografía basada en la posición.

Resumen: En la criptografía basada en la posición el objetivo es establecer una comunicación segura utilizando la localización geográfica de un agente como su única credencial. Esta idea tiene numerosas aplicaciones potenciales (por ejemplo en el campo de los coches autónomos), pero también un interés más fundamental porque presenta una posibilidad de prevenir ataques del tipo main-in-the middle sin necesidad de asumir la existencia de canales autenticados. Además, desde que la criptografía basada en la posición entró en el dominio cuántico hace una década, han aparecido conexiones muy interesantes e inesperadas con áreas como la teoría de la complejidad o la correspondencia holográfica AdS/CFT en el contexto de la gravedad cuántica. En esta charla presentaré una nueva conexión, esta vez con el área del análisis funcional, que nos permitirá utilizar en este contexto una desigualdad de Sobolev debida a Pisier y obtener cotas inferiores a los recursos necesarios para romper la criptografía basada en la posición. (Es un trabajo conjunto con Marius Junge, Aleksander M. Kubicki y Carlos Palazuelos).

Fecha: Jueves, 15 de abril de 2021.

Hora: 12:00 horas.

Webinar: <https://us02web.zoom.us/j/84243517763?pwd=YU9xTnAwR0ZRTGExV3k1WXRENU9ZZz09>

Web: <http://anamat.unizar.es/seminario.html>

<http://eventos.unizar.es/52859/detail/seminario-rubio-de-francia.html>