SEMINARIO

Ignacio Cascudo

IMDEA Software Institute

Esquemas de compartición de secretos verificables "optimistas" con seguridad postcuántica

Abstract: En este trabajo proponemos esquemas de compartición de secretos verificables (''verifiable secret sharing''), que sólo utilizan herramientas criptográficas de clave simétrica (de hecho, oráculos aleatorios, que se pueden implementar con funciones hash), y por tanto ofrecen seguridad postcuántica. En comparación con trabajos previos, nuestro punto de mejora se encuentra en el escenario ''optimista'': si el distribuidor del secreto y todos, salvo un pequeño número, de los receptores de las shares son honestos, entonces nuestro protocolo obtiene importantes mejoras de complejidad. A la vez, nuestro protocolo presenta una complejidad solo ligeramente peor a la del estado del arte en otros escenarios. Nuestra principal herramienta técnica es una prueba de conocimiento cero distribuida de que un polinomio tiene grado pequeño, donde cada uno de los verificadores conoce una evaluación de este polinomio.
Esta charla se basa en un trabajo conjunto con Daniele Cozzo y Emanuele Giunta, publicado en Asiacrypt 24.

Seminario IMUVA, Edificio LUCIA
Jueves 6 de Noviembre de 2025 (13:00)
Organiza: GIR SINGACOM