CONFERENCIA

jueves 7 de junio a las 17h.

aula G3 del Departamento de Matemáticas

Esquemas de compartición de secretos en rampa

Diego Ruano

UNIVERSIDAD DE VALLADOLID

La compartición de secretos (secret sharing) es un método criptográfico para distribuir un secreto entre un grupo de participantes. Cada participante recibe una participación del secreto de forma que éste sólo se puede recuperar cuando un número suficiente de participaciones son combinadas. Los métodos matemáticos incluyen la teoría de códigos lineales y métodos algebraicos. Trabajaremos con esquemas en rampa que permiten reducir el tamaño de las participaciones y veremos su seguridad, sus limitaciones y algunas construcciones.