EL IMUVA OS HABLA

Diego Ruano

Universidad de Valladolid

Esquemas de compartición de secretos en rampa

Abstract: 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.

Sala de Grados I. Facultad de Ciencias
Jueves 20 de Septiembre de 2018 (17:00)
Organiza: GIR SINGACOM