SEMINARIO

Prof. Pedro Chamorro Posada

Univ. de Valladolid

Ataques a sistemas de distribución de clave basados en láseres ultralargos mediante señales de sondeo ocultas

Abstract: Los sistema de distribución de clave basados en láseres ultralargos permiten establecer una clave secreta entre los extremos de una cavidad láser con una extensión de decenas de kilómetros de fibra óptica. Estos sistemas surgen como un método de criptografía basada en principios físicos alternativo a la criptografía cuántica. Siendo de implementación relativamente simple, su seguridad, sin embargo, no se cimenta en principios fundamentales como en el caso de la criptografía cuántica, sino en una asimetría tecnológica, semejante a la asimetría computacional que da soporte a los algoritmos de clave pública, según la cual un atacante necesitaría supuestamente de un equipo altamente sofisticado para comprometer la seguridad del sistema. Este método criptográfico, sin embargo, es potencialmente vulnerable a un ataque activo basado en la utilización de una señal de espectro ensanchado inmersa en el ruido de emisión espontánea de los amplificadores ópticos para sondar el estado del equipo de uno de los usuarios legítimos.

Seminario B118, Facultad de Ciencias
Miércoles 11 de Abril de 2018 (17:00)
Organiza: Física Matemática