Conferencia

Aplicaciones Algebraicas a la Criptografia

Daniel Eduardo Penazzi
Córdoba

Resumen:
A principios de la década del 90 dos ataques devastadores para muchos cifradores vieron la luz: el criptoánalisis diferencial y el criptoanálisis lineal. En el caso del criptoanálisis diferencial se supo entonces que IBM y los servicios secretos de los EEUU en realidad lo conocían desde la década del 70. Este ataque se extendió también a funciones de hash, siendo la principal arma usada en los devastadores ataques de Wang et al de esta década contra los hashes MD5 y SHA-1, usados como estándares.

Veremos como se pueden usar el álgebra (específicamente, los cuerpos finitos) para crear sistemas que sean invulnerables a estos ataques.