SEMINARIO di CRITTOGRAFIA

Tim BEYNE

(KU Leuven)

A GEOMETRIC APPROACH TO SYMMETRIC-KEY CRYPTANALYSIS

---

3 Ottobre 2024

ore 13.30

Via della Vasca Navale 84

AULA C

Abstract: I will introduce the basic principles of the geometric approach to symmetric-key cryptanalysis, first from a general and then from a more concrete point of view. In the main part of the talk, I will survey some applications of the geometric approach to linear, differential and integral cryptanalysis. The emphasis will be on the one-dimensional case. In particular, I will explain how the geometric approach led to the notion of quasidifferential trails in differential cryptanalysis. A few recent applications of quasidifferential trails will be given as examples. Finally, I will introduce a recent extension of integral cryptanalysis (ultrametric integral cryptanalysis) and discuss some of its applications in cryptanalysis and pure mathematics.

per informazioni: Prof. Marco Pedicini