Instituto de Matemáticas

Universidad de Valladolid

CONFERENCIA

Ruud Pellikaan

(Eindhoven University of Technology)

"Error-correcting pairs and majority coset decoding for and from algebraic geometry codes"

Abstract: In this lecture it will be shown how an efficient decoding algorithm can be retrieved from an algebraic geometry code by means of error-correcting pairs and a majority coset decoding scheme, that is without the detour via the representation (X,P,E) of the code, where X is an algebraic curve, P is an n-tuple of mutually distinct points and E is a divisor. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system. In this lecture it will be shown how an efficient decoding algorithm can be retrieved from an algebraic geometry code by means of error-correcting pairs and a majority coset decoding scheme, that is without the detour via the representation (X,P,E) of the code, where X is an algebraic curve, P is an n-tuple of mutually distinct points and E is a divisor. As a consequence algebraic geometry codes with certain parameters are not secure for the code based McEliece public crypto system.

Sala de Grados I de la Facultad de Ciencias
Miércoles 10 de Julio de 2013 a las 12:00

Organiza: Grupo de Investigación SINGACOM