Applying the stuff we like: blocking semiovals and cryptology

Keith Mellinger, University of Mary Washington
Fredericksburg, VA – 22401

Abstract

In 2000, a cryptographic protocol relying on ideas from design theory was patented and gave rise to a whole new set of problems for researchers. The key ingredient was that of a "determining set," something that can be defined completely synthetically. In the case of finite projective planes, an extremal example of a determining set is called a "blocking semioval." In this talk, I will describe the cryptographic protocol from 2000 in detail, providing a firm motivation for the study of blocking semiovals. I will then survey some known results on blocking semiovals and talk about some of my recent work in this area. The techniques involved are a healthy blend of incidence geometry, combinatorics, and algebraic geometry over finite fields.

Keywords: cryptography, combinatorial design, finite projective planes, blocking semiovals.