

1024-14-34

Jose Felipe Voloch* (voloch@math.utexas.edu), Dept. Mathematics, Univ. of Texas at Austin,
1 University Station, Austin, TX 78712. *Symmetric Cryptography and Algebraic Curves.*

The S-boxes of symmetric cryptography can be viewed as polynomials over finite fields (of characteristic two). Their non-linearity properties, which are important for their use in cryptography, translate into properties of certain algebraic curves. I will explain these facts and present some results obtained along these lines. (Received December 08, 2006)