On algebraic problems on finite fields and their importance more than ever in the study of S-boxes in block ciphers

Sihem Mesnager

LAGA (Laboratory of Analysis, Geometry, and Applications), University of Paris VIII, University Sorbonne Paris Nord, and CNRS, Paris, France

Abstract. Throughout this talk, we will place ourselves in finite fields whose theory originates in the work of the French mathematician Evariste Galois. After briefly presenting some main cryptographic problems in symmetric cryptography in the context of block ciphers and highlighting our main motivations, we focus on some underlying fundamental mathematical problems and discuss some algebraic approaches and ingredients used at the core of the methodologies. We shall also present recent achievements in algebraic equations and address open questions, particularly those aimed at implementing methods to solve equations over finite fields and making them available to theorists, notably cryptographers and sequences designers.