Construction of Some Codes Suitable for Countermeasures to Both Side Channel Attacks and Fault Injection Attacks

Ferruh Özbudak
Middle East Technical University, Turkey

Abstract. Using algebraic curves over finite fields we construct some codes suitable for being used in the countermeasure called Direct Sum Masking which allows when properly implemented to protect the whole cryptographic block cipher algorithm against side channel attacks and fault injection attacks simultaneously. This is joint work with Claude Carlet, Cem Guneri and Sihem Mesnager.