Masking With Codes

Shivam BHASIN[1], Claude CARLET[2], Jean-Luc DANGER[1,3],
Sylvain GUILLEY[1,3] and Zakaria NAJM[1]

[1]TELECOM-ParisTech, COMELEC/SEN group
[2]Paris 8 and Paris 13 Universities
[3]Secure-IC S.A.S.

Abstract

Efficient hardware and software masking schemes are analyzed under the view of coding theory.
We show that security and leakage metrics can be expressed solely as a function of the order and the value of the nonzero coefficient having smallest index in the dual distance enumerator polynomial of the code that describes the countermeasure.
Additionally, we prove that the countermeasure figures of merit remain untouched if the leakage is an affine combination of the coordinates of the sensitive variable. However, a statistical study reveals that, in average, a Hamming weight leakage model is less robust.