Optimal Codes for Inner Product Masking

Wei Cheng[1], Sylvain Guilley[1,2], Claude Carlet[3], Jean-Luc Danger[1,2], and Alexander Schaub[1]

[1] LTCI, Télécom ParisTech, Institut Polytechnique de Paris, Paris, France,
[2] Secure-IC S.A.S. Cesson-Sévigné, France
[3] LAGA, Department of Mathematics University of Paris 8, Paris, France
{wei.cheng, sylvain.guilley, jean-luc.danger, alexander.schaub}@telecom-paristech.fr, claude.carlet@univ-paris8.fr

Abstract. Masking is the most popular countermeasure to protect cryptographic implementations against side-channel analysis, since it is provable secure and can be deployed at algorithm level. To strengthen the original Boolean masking scheme, several works have suggested to use more complicated schemes with high algebraic complexity, like affine masking and polynomial masking. Therefore, the *Inner Product Masking* (IPM) was proposed to be a better alternative with its intrinsic algebraic complexity. In this work, we express the security order of generalized IPM schemes from the viewpoint of coding theory, which allows us to optimize it. Specifically, we highlight first that the IPM scheme is not optimal by showing different security order in byte- and bit-level, respectively. In particular, this result confirms the previous observations made by Balasch *et al.* at EUROCRYPT' 15 and at ASIACRYPT' 17 and Poussier *et al.* at CARDIS' 17 regarding the parameters effect in IPM.
More importantly, we characterize this parameter effect by linking the side-channel resistance of IPM to the concept of minimum distance and one coefficient in weight enumeration polynomial of a linear code. The closed-form expression is proposed for depicting the connection, also allows us to systemically choose optimal codes for IPM. As the last contribution, we present the optimal linear code in several scenarios for IPM with two and three shares. The experiments are in perfect accordance with our theoretic analysis and finely demonstrate the optimality of the codes chosen by our method. Our results also present a solid explanation on parameters effect found by Balasch *et al.* and Poussier *et al.*