# A Generic Information-Theoretic Framework for Evaluating the Side-Channel Security of Masked Implementations

Olivier Rioul[1]

Joint work with Julien Béguinot[1], Yi Liu[1], Wei Cheng[1,2], and Sylvain Guilley[1,2]

[1] LTCI, Télécom Paris, Institut Polytechnique de Paris, France
[2] Secure-IC S.A.S., Paris, France

We propose an information-theoretic framework that aims at unifying and optimizing several previous works on the side-channel security of masked implementations of any order $d$ in some Abelian group: Duc *at al.* at EUROCRYPT2015, Dziembowski *et al.* at TCC2016, Chérisey *et al.* at CHES2019, Prest *et al.* at CRYPTO2019, Masure *et al.* at CARDIS2022, Ito *et al.* at CCS2022, Liu *et al.* at ITW2023, and Béguinot *et al.* at COSADE2023 and ISIT2023. In this general framework, two theoretical ingredients are systematically leveraged: (i) a variation of a *Fano inequality* relating the attack performance (success rate) to a measure of information between the sensitive variable and the leakage; (ii) a variation of a *Mrs. Gerber Lemma* lower bounding a statistical measure of the sensitive variable by the product of similar measures for its $d+1$ masking shares. Depending on the choice of the information measure and of the statistical measure, and possibly on Pinsker-type inequalities relating these measures, one can establish anew all previously published lower bounds on the number of queries necessary to achieve a given attack success rate. These results make progress on the evaluation of the security guarantees of higher order masking, and stimulate further research on best possible bounds & possible application to other types of masking schemes.