Taylor Expansion of Maximum Likelihood Attacks, with Application to Masked and Shuffled Implementations

Olivier Rioul[1], Nicolas Bruneau[2],
Sylvain Guilley[1,3], Annelie Heuser[1], and François-Xavier Standaert[4]

[1] LTCI, CNRS, Télécom ParisTech,
Université Paris-Saclay, 75 013 Paris, France.
Email: firstname.lastname@telecom-paristech.fr

[2] STMicroelectronics, 190 Avenue Coq, 13106 Rousset, France.
Email: nicolas.bruneau@st.com

[3] Secure-IC S.A.S., 15 Rue Claude Chappe, Bât. B,
ZAC des Champs Blancs, 35510 Cesson-Sévigné, France.
Email: firstname.lastname@secure-ic.com

[4] UCL Crypto Group, Place du Levant, 3,
B-1348 Louvain-la-Neuve, Belgium.
Email: fstandae@uclouvain.be

The maximum likelihood side-channel distinguisher of a template attack scenario is expanded into lower degree attacks according to the increasing powers of the signal-to-noise ratio (SNR). By exploiting this decomposition we show that it is possible to build highly multivariate attacks which remain efficient when the likelihood cannot be computed in practice due to its computational complexity. The shuffled table recomputation is used as an illustration to derive a new attack which outperforms the ones presented by Bruneau et al. at CHES 2015, and so across the full range of SNRs. This attack combines two attack degrees and is able to exploit high dimensional leakage which explains its efficiency.