SOME RESULTS ABOUT THE DISCTINCTION OF SIDE-CHANNEL DISTINGUISHERS BASED ON DISTRIBUTIONS

Side-Channel Attacks (SCAs) to recover the key of cryptographic implementation consist in distinguishing the correct key from the bad keys hypotheses by selecting the key guess that maximizes a statistical test between the leakage and the sensitive variable.

The Information Theoretic (IT) distinguishers compare the leakage \emph{versus} the leakage conditioned by the sensitive variable, as in the case of the Mutual Information Analysis (MIA). Recently, the Kolmogorov-Smirnov Analysis (KSA) has been proposed as an alternative approach to MIA.

In this talk we will first present another distinguisher, termed Inter-class Information Analysis (IIA). Conversely to MIA or KSA, it consists in comparing the conditional leakages between themselves, pairwise.

Then we will give some comparison results between these different distinguishers, with theoretical and experimental criteria, and for some different types of leakages (especially in the presence of countermeasures to SCA, like masking). Attacks simulations confirm that the new IIA distinguisher compares favorably to MIA and KSA, even when masking is applied to ensure the protection.