# Unprofiled Expectation-Maximization Attack

Julien Béguinot, Wei Cheng, Sylvain Guilley, and Olivier Rioul

Block ciphers are often protected against side-channel attacks by masking. When traces are available for each key hypothesis, the attacker usually resorts to templates attacks with a profiling phase. Lemke-Rust & Paar suggested at CHES2007 a way to profile templates for Gaussian mixture models, with the use of the well-known Expectation-Maximization (EM) algorithm.

In this work, we present a new attack, "unprofiled-EM" (U-EM) that does not use the knowledge of the masks nor requires a profiling phase. This is done by "on-the-fly" regression of the coefficients of a stochastic model using the EM algorithm. Compared to previous methods, it is easy to implement, computationally tractable and efficient in terms of success rate or guessing entropy. We discuss several variations of U-EM and compare their performances on simulations and on real DPA contest traces. The best attack scenario depends on the trade-off between measurement noise and epistemic noise.