Extending the EM injection fault model

S. Ordas, K. Tobich, L. Guillaume-Sage, P. Maurine

The Electromagnetic side-channel has recently been highlighted as an effective medium to inject exploitable faults for physical cryptanalysis. But what type of faults? The literature suggests that EM injections produce timing faults. By using improved equipment and injectors, we revisit this point and we demonstrate that EM injection produces several types of faults. In addition, the local character of EM injection is once again highlighted.