

Reversing the field :  
a single channel for self combined attack  
(to defeat circuit complexity)

Fabien Majéric<sup>1,2</sup>, Eric Bourbao<sup>1</sup> and Lilian Bossuet<sup>2</sup>

<sup>1</sup> Security Labs, GEMALTO (La Vigie),  
Av. du Jujubier, Z.I Athélia IV,  
13705 La Ciotat, Francey

<sup>2</sup> Univ. Lyon, UJM-Saint-Etienne, CNRS,  
Laboratoire Hubert Curien UMR 5516,  
F-42023, Saint-Etienne, France

**Abstract**

With large and complex circuits, finding the good location for fault injection like laser or electromagnetic (EM) injection is challenging and it requires a significant amount of time. We propose a methodology which optimize the research of the right location by exploiting the combined properties of EM emission and EM injection. Moreover, the complex problem for attacking SoC is also discussed through an example and techniques for efficient analysis are also proposed.