Horizontal Attacks in Practice

Ibrahima Diop[1,4], Yanis Linge[1],
Pierre Yvan Liardet[1], Thomas Ordas[1], and Philippe Maurine[2,3]

[1] STMicroelectronics, Rousset
[2] LIRMM, Université Montpellier II
[3] CEA 880 route de Mimet, 13541 Gardanne
[4] Ecole des Mines de Saint-Etienne (EMSE)

Abstract. Nowadays horizontal or one shot attacks theoretically constitute a real threat to the smartcards. Nevertheless, in practice their application remains very difficult due to the environmental countermeasures introduce by designers but also to the complexity of the attacks. Horizontal attacks are constituted of multiple steps. Each step is crucial and can lead to a unsuccessful attack. In a first step the whole curve have to be acquired, then the curve is cut and the different parts have to be synchronized. Finally after a noise reduction and points of interest (PoIs) definition, different distinguishers can be used to retrieve the secret. In this context, this talk proposes effective solutions for their different steps that constitute an horizontal attack in practice.