Algorithmic Approaches to Defeat Side Channel Analysis

Emmanuel Prouff

To defeat Side Channel Analysis, a common countermeasure consists in randomly splitting every sensitive intermediate variable occurring in the computation into several shares and the number of shares, called the masking order, plays the role of a security parameter. Several masking schemes, applicable for arbitrary orders and arbitrary function, have been recently introduced. During this talk, I will present and compare some of the state-of-the art methods and the techniques used to analyse their security. I will also discuss some open issues and present ideas which could be developed to (hopefully) solve them.