On the Machine Learning Techniques for Side-channel Analysis

Stjepan Picek, Annelie Heuser, Sylvain Guilley,

Domagoj Jakobovic and Nele Mentens

Abstract. Side-channel attacks represent one of the most powerful cat-egory of attacks on cryptographic devices with profiled attacks in a prominent place as the most powerful among them. Indeed, for instance, template attack is a well-known real-world attack that is also the most powerful attack from the information theoretic perspective. On the other hand, machine learning techniques have proven their quality in a numer-ous applications where one is definitely side-channel analysis, but they come with a price. Selecting the appropriate algorithm as well as the parameters can sometimes be a difficult and time consuming task. Nev-ertheless, the results obtained until now justify such an effort. However, a large part of those results use simplification of the data relation from the one perspective and extremely powerful machine learning techniques from the other side. In this paper, we concentrate first on the tuning part, which we show to be of extreme importance. Furthermore, since tuning represents a task that is time demanding, we discuss how to use hyperheuristics to obtain good results in a relatively short amount of time. Next, we provide an extensive comparison between various ma-chine learning techniques spanning from extremely simple ones (even without any parameters to tune), up to methods where previous expe-rience is a must if one wants to obtain competitive results. To support our claims, we give extensive experimental results and discuss the neces-sary conditions to conduct a proper machine learning analysis. Besides the machine learning algorithms' results, we give results obtained with the template attack. Finally, we investigate the influence of the feature (in)dependence in datasets with varying amount of noise as well as the influence of feature noise and classification noise. In order to strengthen our findings, we also discuss provable machine learning algorithms, i.e., PAC learning algorithms.