Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Dimensionality Reduction Methods for Side-Channel Attacks - A Survey

Even though a cryptographic algorithm is proven to be mathematical secure for the best known attack, its implementation can lead to a so called side-channel. An example for such a channel is the power consumption or the EM emissions of the executing device. With side-channel analysis (SCA) the additional information of a power side-channel can be exploited to extract the secret key and therefore break the cryptosystem.

On challenge during the practical execution of SCA attacks consists in handling the huge amount of measurement data that is often needed in order to execute a successful attack. In order to reduce data complexity and therefore the amount of data that has to be processed for an attack, different dimensionality reduction methods can be used. A prominent example for such a method is the Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA).

This work should provide a survey of different dimensionality reduction methods in the context of SCA. A focus should lie on PCA and LDA but an extensive literature review should be performed. As a starting point the reference [1] can be used. Advantages and disadvantages as well as the field of application of each method should be discussed.

[1] Cagli et al.: “Enhancing Dimensionality Reduction Methodsfor Side-Channel Attacks”, International Conference on Smart Card Research and Advanced Applications (CARDIS), 2015

Contact

Request the shown topic

Advisors

Thomas Schamberger