Enhancing SIFA

Statistical Ineffective Fault Attacks pose a serious threat to the implementation of cryptographic algorithms due to the relaxed fault model.
Usually the SEI is used as a metric to distinguish the correct target partial subkey.
In this work other possibilities to find the correct target partial subkey should be evaluated (analytic approaches, statistical approaches, and machine learning)


The information about the work is deliberately kept short, for detailed information I am personally available at any time.

Prerequisites

- Python
- Basic Knowledge Statistics
- Basic Knowledge Machine Learning

Advisors

Michael Gruber