FP/BA/MA:
Extending the XFC-Framework to Sponge cryptography

Description:
Fault attacks pose a serious threat to the implementation of cryptographic algorithms, as they can be performed using even low cost equipment [1]. Finding a fault attack is usually a tedious and rather time-consuming task. To automate this task the XFC framework [2] was developed. This framework uses so called colours to trace the fault propagation through the cipher. Your objective would be at first to implement the XFC framework in a high level language (Python), and later on check if it is possible to extend the framework to sponge cryptography or write a new framework from scratch using the principles of [2].

References


Please apply to:
Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
M.Sc. Michael Gruber
Theresienstraße 90
80333 München
or via email: m.gruber@tum.de

Visit us at https://www.sec.ei.tum.de/