Cryptographic Engineering

The Cryptographic Engineering group is currently in its incubation stage, consisting of 6 researchers. Our focus is on all aspects of cryptographic engineering, and in particular on side-channel and fault analysis.

Mission

It is our mission to enhance knowledge in the area of Side-Channel Analysis on cryptographic devices. To achieve this goal we will develop new analysis methods and countermeasures using cutting-edge equipment and collaborate with top research institutes worldwide.

Vision

We envision to lay the foundations of state-of-the-art research in constructive Side-Channel Analysis and Secure Design in Singapore.

Ongoing Project: Physical Analysis and Cryptographic Engineering

While cryptographic algorithms (required nowadays in virtually all forms of electronic communications) can be designed provably secure, their implementations usually leak information about the data processed via so-called side-channels (e.g. timing behavior and power consumption of the platform device), which eventually can lead to a security breach of the whole system. Even worse, it is also possible to alter the operating conditions of the device, e.g. by inducing a voltage glitch, or to introduce faults by a laser to cause erroneous behavior, which allows leakage of more information.

These physical analysis in fact constitute the weakest link in a secure system and pose a great challenge for designers.