
- Master-/Diplomthesis - Physical attacks and code-based cryptosystems

CASED	Das Center for Advanced Security Research Darmstadt (CASED) bündelt die Kompetenzen der Technischen Universität Darmstadt, des Fraunhofer-Instituts für Sichere Informations-technologie und der Hochschule Darmstadt. In einer Kooperation von Informatikern, Ingenieuren, Physikern, Juristen und Betriebswirten sowie mit internationalen Forschungszentren und Industriepartnern, erforscht CASED zukunftsweisende IT-Sicherheitslösungen, entwickelt diese und bringt diese in die Anwendung und wirtschaftliche Verwertung. Mehr Informationen unter www.cased.de .
Hintergrund	Code-based cryptography is one of the branches of post-quantum cryptography. Schemes based on problem has syndrome decoding or decoding random codes are well studied for years. To consider the use of code-based cryptosystems in the real life, they must be resistant to physical attacks. To date, the study of such attacks on such schemes are rare. Both practical and theoretical, this thesis proposes to study the physical attacks also called side-channel attacks (SPA, DPA, Fault Attack) and show how we can apply these patterns to attack code-based cryptosystems (CFS, Stern, McEliece).
Voraussetzungen	<ul style="list-style-type: none">• High motivation and creativity• Skills in C• Good knowledge of cryptographic constructions• Experience with reading research papers.
Einstellung	<ul style="list-style-type: none">• Immediately
Kontakt	Dr. Pierre-Louis Cayrel pierre-louis.cayrel@cased.de CASED - Center for Advanced Security Research Darmstadt Mornwegstraße 32 64293 Darmstadt