

---

# - Master/Diploma thesis -

## Algebraic cryptanalysis of light-weight block ciphers

---

### CASED

In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on [www.cased.de](http://www.cased.de).

### Motivation & Goal

Recent boost in using cheap and low-resource RFID-tags poses new tasks for symmetric cryptography. The fact that such RFID-tags only have very limited space and computing power makes using standard (block) ciphers impossible. A new trend in the cipher design in the recent years has been to provide so-called light-weight block ciphers especially designed for usage in resource constraint devices. The goal is to provide adequate security, but with as simple and few operations as possible. As a consequence, cryptanalytic techniques should be taken into account very carefully for such light-weight ciphers. In particular, algebraic attacks make use of a simplified structure of non-linear components (S-Boxes). The goal of the thesis is, basing on some previous results, explore resistance of certain light-weight ciphers (e.g. SEA, KTAN, PRINT-Cipher) against algebraic attacks. Tools from computer algebra, such as Magma, PolyBoRi, SAT-solvers are to be used within this project.

### Requirements

- High motivation and creativity;
- Good knowledge of symmetric cryptography and block cipher design;
- Knowledge of algebraic cryptanalysis is a plus;
- Experience with reading research papers;

Knowledge of the English language goes without saying.

### Contact

If you are interested, please contact Dr. Stanislav Bulygin  
Location: CASED, 4.3.29  
E-mail: Stanislav.Bulygin@cased.de