

---

## - Bachelor thesis -

# SAT-solving in algebraic cryptanalysis

---

### 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

Satisfiability (SAT) problem is one of the most important problems in theoretical computer science. The problem is to determine whether there exists an assignment of variables in a Boolean formula that evaluates this formula to TRUE. SAT problem and SAT-solving (finding an assignment evaluating to TRUE) has numerous applications in different areas of computer science. Recently SAT-solvers have found their applications in algebraic cryptanalysis of stream and block ciphers. The goal of this work is to provide a comprehensive overview of SAT-solvers especially in relation to algebraic cryptanalysis. In particular the SAT-solvers MiniSAT2 and CryptoMiniSAT2 are to be investigated using specific cryptanalytic problems as case studies. One of the goals of this work is to determine parameters and conversion techniques that make usage of SAT-solvers in algebraic cryptanalysis optimal.

### Requirements

- High motivation and creativity
- Good knowledge of symmetric cryptography and ciphers design
- Knowledge of algebraic methods for system solving is a plus
- Knowledge of SAT-solving techniques 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, 4.3.03

E-mail: [Stanislav.Bulygin@cased.de](mailto:Stanislav.Bulygin@cased.de)