
- Bachelor thesis -

Cube attacks with non-linear relations

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.

Motivation & Goal

Cryptanalysis of cryptographic primitives like block and stream ciphers is important in assessing their security and possible weaknesses. The cube attack of Dinur and Shamir (also known as AIDA by ...) is a method of attacking cryptographic primitives considered as a black box. The method showed its particular efficiency applied to stream ciphers, like Trivium. The idea of the cube attack is to obtain linear relations in unknown key via summing the black box function over certain public values called cubes. The goal of the thesis is to investigate a possibility of using non-linear, in particular quadratic and cubic, relations and not only linear. After working out some artificial examples to understand the concept, applications to modern stream ciphers, e.g. Trivium are to be undertaken. Computer algebra systems like Magma and SAGE/PolyBoRi are to be used for solving non-linear systems arising in the new method.

Requirements

- High motivation and creativity;
 - Good knowledge of symmetric cryptography and ciphers design;
 - Knowledge of algebraic methods for system solving 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