Cryptanalysis using constraint programming solvers: the case of cube attacks

Laboratory, institution and university The internship will be located at IRISA (Rennes).

Team or project of the Lab Team EMSEC at IRISA

Name and email address of the advisor Stéphanie Delaune, Stephanie.Delaune@irisa.fr and Patrick Derbez, Patrick.Derbez@irisa.fr

Indemnisation The internship is supported by the European grant **POPSTAR** (ERC Starting Grant) and the ANR grant **CryptAudit**.

Keywords cryptanalysis, constraint programming, hash function

Context. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Cryptography prior to the modern age was synonymous with encryption, the conversion of information from a readable state to apparent nonsense, but nowadays many other cryptographic primitives exist with various goals. Cryptanalysis aims at testing whether the properties that a primitive is supposed to achieve are actually guaranteed.

Nowadays, the cryptanalysis progress of cryptographic primitives heavily depends on automated evaluation tools, and providing a reliable security evaluation of these primitives is of paramount importance. Many classical cryptanalysis methods can actually be converted into mathematical optimisation problems. This subsequently paved the way to the use of automated tools such as SAT solvers, Mixed-Integer Linear Programming (MILP), or Constraint Programming (CP) to solve these problems.

Objectives of the internship. The goal of this internship is to do cryptanalysis relying on constraint programming models. The aim is to see whether constraint programming solvers that are more expressive than SAT solvers or MILP are suitable for this task.

To start, the intern will analyse Keccak which has been designed by Bertoni et al. [1] and which has been selected as the new cryptographic hash function standard SHA-3. The intern will focus on a particular class of attack, namely cube attacks. Cube attack is an efficient key-recovery attack proposed at Eurocrypt in 2009 [2]. This type of attacks has been analysed in [1] relying on MILP. Since constraint programming has been already proved useful to solve several cryptanalytic problems, such as the chosen key differential attack against the standard block cipher AES [3], we would like to investigate how constraint programming solvers behave regarding this class of attacks.

Expected skills. We are looking for candidates with good skills in Foundations of Computer Science (logic, automatic deduction, ...). Some knowledge in security is an asset but is not mandatory. The candidate will assimilate this knowledge during the internship.

[1] https://keccak.team/index.html

Références

[1] Wenquan Bi, Xiaoyang Dong, Zheng Li, Rui Zong, and Xiaoyun Wang. Milp-aided cube-attack-like cryptanalysis on keccak keyed modes. Cryptology ePrint Archive, Report 2018/075, 2018. `https://eprint.iacr.org/2018/075`.

[2] Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. In *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, pages 278–299, 2009.

[3] David Gerault, Marine Minier, and Christine Solnon. Constraint programming models for chosen key differential cryptanalysis. In *Principles and Practice of Constraint Programming - 22nd International Conference, CP 2016, Toulouse, France, September 5-9, 2016, Proceedings*, pages 584–601, 2016.