Offer of 1 year Post-doct Position
Constraint Programming for Cryptanalysis of Symmetric Encryption Schemes

November 27, 2018

Supervisor: Pascal Lafourcade
Location: LIMOS, Clermont-Ferrand, France
Salary: 2000 euros
Duration: 1 year
Starting date: As soon as possible, when we have a good candidate.
Your Profile:

- A PhD in Computer Science, Applied Mathematics, Cryptography or related field.
- Competitive research record in symmetric cryptography or in constraint programming.
- Commitment, team working and a critical mind.
- Fluent written and verbal communication skills in English are essential

Application: Send by email at `pascal.Lafourcade@uca.fr` your cover letter, your CV, your PhD, reports of the reviewers of your PhD, a slection of your best papers related to the post-doc offer, some recommandation letters, contact information for 3 referees and any information that might help us to chose you.

1 Context

This post-doc is founded by the ANR project Decrypt starting in January 2019. This project involves Université de Lorraine/LORIA, Université Rennes 1/IRISA, ARMINES/TASC (IMT-Atlantique/Université Nantes) and Université de Lyon (INSA de Lyon /Université Lyon 1)/LIRIS

Symmetric cryptography is a cornerstone of everyday digital security. Contrary to public key cryptography, the two parties must share a common key to communicate. The most common primitives in symmetric cryptography are stream ciphers, block ciphers that guarantee confidentiality of communications and hash functions for integrity. Thus, for securing our everyday life communication, it is necessary to be convinced by the security level provided by all the symmetric key cryptographic primitives.

During the last five years, many research results [1, 5, 4] have tried to attack those primitives using automatic tools such as Mixed Integer Linear Programming (MILP) or Boolean satisfiability (SAT) solvers. However, transforming a theoretical cryptanalysis into a SAT problem or into a set of linear constraints could be a hard and time-consuming task. Our aim is to use constraint programming (CP) to simplify the way the symmetric key attacks are modeled and thus to overpass existing cryptanalytic results. Preliminary studies [6, 2, 3] are really encouraging.

2 Goal

The goal is to study the capabilities of CP, SAT and MILP solvers to solve cryptanalytic problems. A cryptanalytic problem contains two components. The first component is the symmetric key scheme itself, like for instance AES. The second component is the kind of attacks that is considered such as, for example, cube attacks, conditional cube

attacks with division property, (related-key) differential and linear cryptanalysis against block cipher schemes, word-based division property / integral distinguisher.

The main goal is to identify schemes and attacks for which it is possible to use off-the-shelf CP, SAT or MILP approaches. To achieve this goal, teh work will be divided into the following tasks.

1. **Task 1.1:** Design CP, SAT, and MILP models for cryptanalytic problems. We will mainly focus on the following attacks: cube attacks, conditional cube attacks with division property, (related-key) differential and linear cryptanalysis against block cipher schemes, word-based division property / integral distinguisher. This task requires close interactions between members of the CP community and members of the symmetric cryptographic community. CP models will be defined using existing modeling languages such as XCSP and MiniZinc. SAT and MILP models will be either designed directly, or via CP modeling languages such as Picat (that can automatically generate SAT or MILP models from CSP models). Of course, we will rely on existing models whenever they already exist.

2. **Task 1.2:** Experimentally evaluate CP, SAT, and MILP solvers on the models designed in Task 1.1, and compare these solvers with existing dedicated cryptanalysis approaches. Our main performance criteria will be the solving time and the memory consumption. For optimization problems, we may also compare computed bounds within given time limits as existing solvers may not always be able to find optimal solutions and prove optimality.

3. **Task 1.3:** Study symmetric encryption schemes and identify for several schemes the different components that are used in the scheme design. For instance many schemes use XOR operations or S-Boxes but some use modular addition or multiplication. This should allow us to identify recurring sub-problems. Those sub-problems could be modeled as subsets of constraints and we could facilitate the way we model them and the way we solve them by defining new global constraints.

References

[1] C. Cid, T. Huang, T. Peyrin, Y. Sasaki, and L. Song. A security analysis of deoxys and its internal tweakable block ciphers. *IACR Trans. Symmetric Cryptol.*, 2017(3):73–107, 2017.

[2] D. Gerault, M. Minier, and C. Solnon. Constraint programming models for chosen key differential cryptanalysis. In *Principles and Practice of Constraint Programming - CP 2016*, volume 9892 of *LNCS*, pages 584–601, 2016.

[3] D. Gerault, M. Minier, and C. Solnon. Using constraint programming to solve a cryptanalytic problem. In *26th International Joint Conference on Artificial Intelligence, IJCAI*, pages 4844–4848, 2017.

[4] S. Huang, X. Wang, G. Xu, M. Wang, and J. Zhao. Conditional cube attack on reduced-round keccak sponge function. In *Advances in Cryptology - EUROCRYPT 2017*, volume 10211 of *LNCS*, pages 259–288, 2017.

[5] Y. Sasaki and Y. Todo. New impossible differential search tool from design and cryptanalysis aspects - revealing structural properties of several ciphers. In *Advances in Cryptology - EUROCRYPT 2017*, volume 10212 of *LNCS*, pages 185–215, 2017.

[6] S. Sun, D. Gerault, P. Lafourcade, Q. Yang, Y. Todo, K. Qiao, and L. Hu. Analysis of aes, skinny, and others with constraint programming. *IACR Trans. Symmetric Cryptol.*, 2017(1):281–306, 2017.