Practical integral attacks on the PRESENT block cipher

Ivaylo Krumov
BSP 3 - BiCS Semester 3 (2022-2023)
ivaylo.krumov.001@student.uni.lu

Project objectives

The overall goal of this project is to explore the basics of cryptography and cryptanalysis with the objective to implement some practical attacks (called integral attacks) on a (reduced) version of the PRESENT block cipher (i.e. an encryption algorithm), as well as the use of some automated tools like Mixed Integer Linear Programming (MILP).

Scientific objectives

The scientific part of the project aims to answer the question “How many rounds of the PRESENT block cipher can be attacked using integral attacks with practical complexity?”. The scientific deliverable will complement the technical one by acting as its theoretical counterpart and each of them will provide an answer to the scientific question in one way or another. Alongside the answer, the scientific deliverable is expected to give insight into the domain of cryptography and cryptanalysis and inform about the essence of the PRESENT block cipher and integral attacks, as well as how to search for these attacks using automated tools like MILP.

Technical objectives

For the technical portion of the project, the goal is to provide an implementation of an algorithm for a specific type of cryptanalytic attack called integral attack. The attack is aimed towards the PRESENT block cipher, which will need to be implemented beforehand. The algorithm is expected to be able to attack a reduced version of the cipher within practical complexity (i.e. in such a way that it can be easily conducted on a regular laptop). The purpose of the integral attack will be to retrieve the cipher’s master key on several rounds of the cipher - beginning from 5 up to as many as possible given the practical technical constraints. The results from the technical deliverable will also complement the scientific deliverable and will be used to give a concrete answer to the scientific question.

Project description

Prerequisites

The complete realization of the project, both the scientific and technical deliverables, will require the possession of several skills and competencies. The following is a brief list of these prerequisites:

- Basic theoretical knowledge about cryptography and cryptanalysis
- Knowledge about the PRESENT block cipher, integral attacks and MILP
- Experience in programming using Python
- Ability to work with automated tools for MILP optimization, specifically the use of Gurobi to implement higher round integral attacks

Scientific deliverable

To adequately answer the scientific question “How many rounds of the PRESENT block cipher can be attacked using integral attacks with practical complexity?”, research will be done in order to understand the essence of the question and its key terms. To achieve this, relevant information will be used from the following scientific papers:

- PRESENT block cipher specification: **Bogdanov, A. *et al.* (2007). PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds) Cryptographic Hardware and Embedded Systems - CHES 2007. CHES 2007. Lecture Notes in Computer Science, vol 4727. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74735-2_31**
- First presentation of an integral attack (although on a different cipher): **Daemen, J., Knudsen, L., Rijmen, V. (1997). The block cipher Square. In: Biham, E. (eds) Fast Software Encryption. FSE 1997. Lecture Notes in Computer Science, vol 1267. Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0052343**
- Description of using MILP and division property to modernize integral attacks: **Xiang, Z., Zhang, W., Bao, Z., Lin, D. (2016). Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers. In: Cheon, J., Takagi, T. (eds) Advances in Cryptology – ASIACRYPT 2016. ASIACRYPT 2016. Lecture Notes in Computer Science(), vol 10031. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-53887-6_24**
- Description of an attack on 5 rounds of PRESENT privately communicated by the tutor

The mentioned research will consist of gaining an understanding of the scientific question through the information provided in these papers. This will be vital in order to give a proper answer to it, which will be formulated mainly using the explored information from all papers alongside the results from the technical part of the project.

Technical deliverable

The technical deliverable will be presented in the form of an algorithm that will be able to perform an integral attack on a reduced implementation of the PRESENT block cipher. Both the cipher implementation and the integral attack algorithm will be written in Python. Initially, the algorithm will be dedicated to attacking the cipher with an encryption over 5 rounds. To optimize the algorithm for attacks on a higher number of rounds, the use of MILP will be included via automated tools. In particular, the Gurobi Optimizer tool will be utilized to efficiently search for higher round integral attacks. The ultimate goal will be to successfully do an integral attack on as many rounds of the cipher as possible within a practical amount of time and complexity. The produced results will be used to directly contribute to answering the scientific question.