Decoding Random Linear Codes

Final version of the project's subject description

Project main objectives

For the 5th semester, with the guidance of my tutor, we would try to dig a little deeper in the scientific area of cryptography. These days, one of the most crucial subjects, which also reflects on our everyday life, is security and especially online security. Quantum computers are becoming more and more used by huge companies, making security provided by the current algorithms less dependable and reliable. Algorithms built on integer factorization, discrete logarithms problems or elliptic curves are vulnerable to quantum computers. Therefore, the objective of this project is to study, focus on and further expand my knowledge about the post-quantum cryptography, or quantum safe as it is widely known. For that task, it is also important, as objective, to implement some of the basic cryptographic tools and algorithms, to further practice and understand the scientific part. The main scientific area of the project focuses on linear codes.

Main competencies

In order to get started with this project, some main - minimum competencies must be owned. First of all, for the scientific part and also later, for the implementation, the student needs to have basic knowledge of the elementary linear algebra. This mainly includes matrices and vector multiplication, Gaussian elimination and solving linear equations. Furthermore, an understanding of modular arithmetic would be an extra advantage. For the technical part, algorithmic thinking and how to implement it in a program is more than important. Finally, good programming skills are always important and because of the nature of the BSP, the project's implementation uses Sagemath and Python. Therefore any knowledge of those two, could be helpfull and an advantage for the progress of the whole project.

Scientific Deliverable description

For the scientific part of this project, I am going to study the case of linear codes and their decoding techniques. Linear codes, in coding theory, are the error-correcting codes that are using matrices(therefore linear) to produce codewords. Because of the notion of syndrome decoding, linear codes are way more efficient at encoding and decoding, which make them very useful in error correction of codewords. That is why they are being used in communication channels, in order to make it easier to correct some errors (depending on the weight) of the codewords. The first part of the scientific section of the

paper is dedicated to explaining in detail what linear codes are and how they are being defined. Furthermore, as we progress further, the paper will focus on some decoding methods, like the combinatorial and the birthday. As mentioned in the BSP Declaration, and remains the main objective of the scientific part, to get a glimpse on the modern encryption and linear codes, understand different approaches of decoding and comprehend the relations of the problem to code based encryption.

Technical deliverable description

For the technical deliverables, the things are pretty straight forward, following the steps of the scientific part. The goal is to produce a program using the programming language Python integrated with Sagemath, that handles the encoding and decoding of messages and codewords respectively. As mentioned, different methods of decoding will also be used in order to achieve more efficiency and reduce outcomes. The program should include a few algorithms, from trivial to efficient ones, so that the performance improvements would be noticeable. Finally, as always, if there is enough time left and the necessary theoretical and technical parts are covered, additional optimization and expansion of the project will be offered.

References

- Lectures about codes & decoding, including combinatorial & birthday decoding: https://www.canal-u.tv/chaines/inria/3-message-attacks-isd
- Slides about decoding: https://nis-summer-school.enisa.europa.eu/2018/cources/PQC/12-enisa18_loebenberger.pdf
- Sagemath documentation for matrices and vectors
- Guiding emails with educational material