Decoding Random Linear Codes

Final version of the project's subject description

Project main objectives

For the 5th semester bachelor project, this paper intends 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 the currently acquired knowledge about the post-quantum cryptography, or quantum safe as it is widely known and especially a sub domain that of linear codes, which is the main scientific subject. Decoding random linear codes is a hard (NP-complete) problem. 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.

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, it is going to be studied 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, modular arithmetic (finite field

GP(p), the problems of decoding a linear code are and how those are being defined. Additionally, this paper studies the syndrome decoding, small instances of the decoding problem, large distances and their difficulty, how all of these are used in cryptography and how they are related to post-quantum cryptography. Equivalence between decoding and low-weight codeword problem and interpolation with errors by code decoding are also examined. Furthermore, as this project progresses further, the paper will focus on some algorithms of decoding methods, like the combinatorial, the birthday and more. 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, by implementing basic or moderate algorithms. These algorithms are feasible and concern small-sized codes, allowing us to estimate security of cryptosystems. First, it is vital to start by implementing basic functions to work with linear codes like generating random linear code, encoding - decoding error free messages, adding random errors and computing the syndrome. Commencing, there is the implementation of the decoding algorithms concerning words with given errors. Some of those are; the combinatorial enumeration, Birthday decoding, Prange algorithm and more. One of the goals is to provide a kind of comparison between those algorithms based on several parameter sets (n,k). 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

- Eugene Prange. The use of information sets in decoding cyclic codes. IRE Transactions on Information Theory, 8(5):5-9. 1962.
- P. J. Lee, E. F. Brickell. An observation on the security of McEliece's public-key cryptosystem. EUROCRYPT'88. 1988.
- J. S. Leon. A probabilistic algorithm for computing minimum weights of large error correcting codes. IEEE Transactions on Information Theory, 34(5):1354-1359. 1988.
- A. Canteaut, F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. IEEE Transactions on Information Theory, 44(1):367-378. 1998.
- R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. In Jet Propulsion Laboratory DSN Progress Report 42-44, pages 114-116, 1978.
- F.J. MacWilliams, N.J.A. Sloane. The Theory of Error Correcting Codes. NorthHolland, 1977.
- Daniel Loebenberger. Code-based Cryptography, a Hands-On Introduction. September 2018. https://nis-summer-school.enisa.europa.eu/2018/cources/PQC/12-enisa18_loebenberger.pdf

- Sendrier Nicolas, Marquez-Corbella Irene, Finiasz Matthieu, Lectures on several topics of cryptography. https://www.canal-u.tv/chaines/inria/3-message-attacks-isd
- Andre Esser, Emanuele Bellini. Syndrome Decoding Estimator.Technology Innovation Institute, UAE. https://eprint.iacr.org/2021/1243.pdf
- Sagemath documentation for matrices and vectors.
- Guiding emails with educational material from tutor.