Gymnasium der Freien Katholischen Schulen Zurich
University of Zurich
Institute of Mathematics

FKS^z Gymnasium 100 FKS^z Jahre

Some Applications of Algebra in Coding Theory and Cryptography

Author:
Constantin V. A. Vlachos

Supervisor:
Niklas Gassner

First Project

1.1. Goal. In this experiment it was our goal to experimentally find the parity check matrix of the ISBN code (International Standard Book Number).

1.2. Method. We assumed the ISBN code was a linear subspace of $\mathbb{F}_{11}^{10}$ of unknown dimension $k < 10$. The strategy employed was to first find a generator matrix, as we had a large amount of codewords (ISBN numbers) at our disposal that we could use as rows of a generator matrix. We began by assuming $k = 1$ and constructed a potential generator matrix G_1, a 1×10 matrix over $\mathbb{F}_{11}$. Next, we attempted to find a codeword c that did not lie in the rowvectorspace of G_1. We concluded that $k \neq 1$ and assumed $k = 2$. We chose our new potential generator matrix, G_2, to simply be the 2×2 matrix, whose first rowvector was the rowvector of G_1 and second rowvector was simply c, as this left G_2 with a full rank. We repeated this process for $k = 1, ..., 8$.

1.3. Results. After constructing matrices of ranks 1 till 8 and still finding codewords that did not lie in their rowvectorspace, we concluded that the rank of the generator matrix of the ISBN code equals 9, i.e. $k = 9$. We then proceeded to compute the parity check matrix from the generator matrix. Finally, we found that the parity check matrix H of the ISBN code was

$$H = \begin{pmatrix} X & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Second Project

2.1. Goal. In the second experiment we researched the IBAN code (International Bank Account Number). We stated and proved our own theorem that the IBAN code is single error detecting.

2.2. Method. In order to prove our theorem, we presented the reader with *p-adic numbers* and showed their construction from the rationals. These would become instrumental in the proof of our theorem. Then we also introduced PDIBANs, IBANs post permutation and decoding of certain letters and digits. Finally, we came up with a simple decoding algorithm using PDIBANs and their *p-adic* representation to show that the IBAN code is indeed single error detecting.

2.3. Results. We found that the IBAN code is not linear and that it detects all single errors.

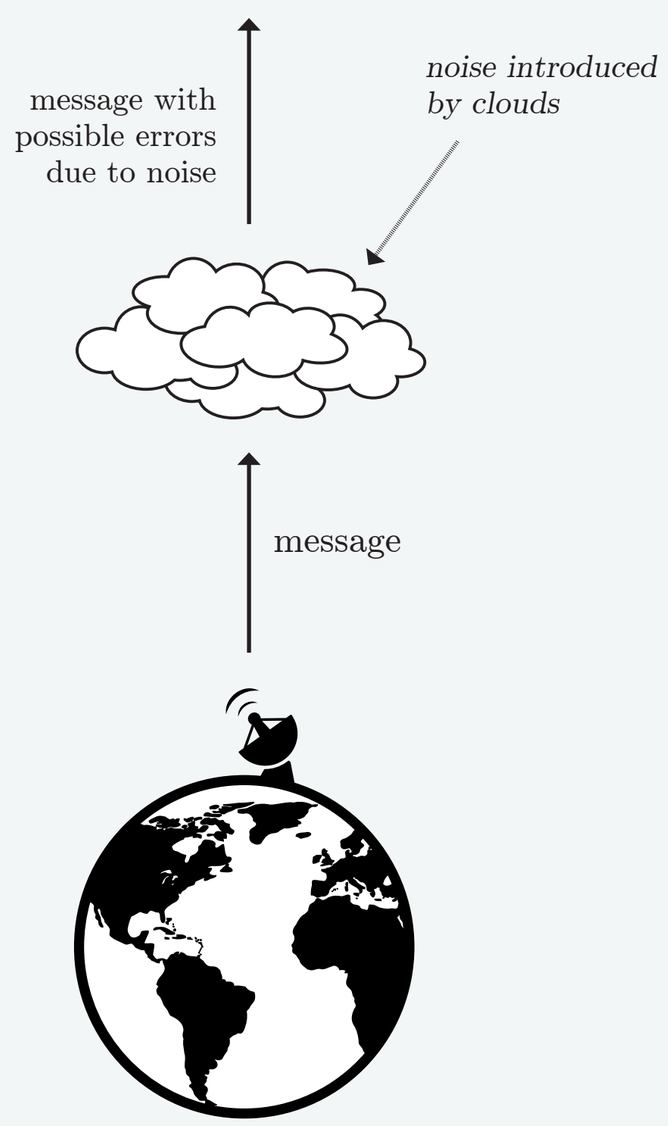
Third Project

3.1. Goal. The goal of the final experiment of this project was to create our own hash function, where we specifically focused on pre-image resistance and second pre-image resistance.

3.2. Method. We created our own pseudo-random generator, which we then used as the required pseudo-random generator in Goldreich, Goldwasser and Micali's construction of a pseudo-random function (1986). This function was then used in our hashing algorithm. After constructing the hash function we attempted to break its second pre-image resistance and pre-image resistance with a few standard attacks.

3.3. Results. We found that the hash function first proposed in the paper had some major pre-image resistance issues that we then proceeded to fix. We also saw that constructing a hash function with PRG's and PRF's is very much possible.

Coding Theory



Cryptography