SageMath Toolbox for Rank Error-Correcting Codes

Research Internship with Dr. Simona Samardjiska

Maaike van Leuken BSc

M.vanLeuken@student.ru.nl

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

March 5th 2021

Introduction

- Quantum computing breaks
  - Integer factorization problem $\rightarrow$ RSA
  - Discrete logarithm problem $\rightarrow$ ElGamal, ECC
- (General) Syndrome Decoding Problem (NP-hard)
- Rank Syndrome Decoding Problem!

Background

Error-Correcting Codes

An $[n, k]-$code $C \subseteq \mathbb{F}_{q^m}$ has

- Generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$
- Parity check matrix $H \in \mathbb{F}_{q^m}^{(n-k) \times n}$
- Messages $m \in \mathbb{F}_{q^m}^{k}$
- Codewords $c \in \mathbb{F}_{q^m}^{n}$

Properties: $GH^T = 0$, $Hc^T = 0$
Encoding: $c = mG$
Syndrome decoding: $s(y) = Hy^T = H(c + e)^T = He^T$

Background

Rank

$c = (z_2, z_2 + 1)$ in $[2, 1]-$code $C \subseteq \mathbb{F}_{2^2}$ in matrix form: $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$

$\rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow |c|_R = 2$

Support

$Supp(c) = \langle z_2, z_2 + 1 \rangle_2$ is the subspace with basis $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Syndrome Decoding Problems

Rank Syndrome Decoding (RSD) Problem

$$\begin{cases} He^T = s^T \\ |e|_R = w \end{cases}$$

Knowing s and $E = Supp(e)$ gives e!

bit security	128	192	256	
RSA	3 072	7 680	15 360	IF
Goppa-McEliece	$2 \cdot 10^6$	$4 \cdot 10^6$	$6 \cdot 10^6$	GSD
Gabidulin (DRANKULA)	62 000	118 160	216 000	RSD
QC LRPC (LOCKER)	5 893	8 383	9 523	RSD

Toolbox

- In SageMath
- Basics:
  - Support
  - Finding codewords
  - Rewriting elements in certain basis
- Attack: GRS algorithm
- Family of codes: LRPC codes

GRS Algorithm

1. Pick $F \subseteq \mathbb{F}_{q^m}$ of dimension r
2. Rewrite $He^T = s$, where e is rewritten in F via $e_i = \sum_{j=0}^{r-1} \lambda_{ij} F_j$, nr unknowns
3. Rewrite system, where H, F and s are rewritten in basis, gives $(n-k)m$ equations
4. Find solution, check rank

Low Rank Parity Check (LRPC) Codes

- Construction: pick d random vectors for F, find H
- Encoding: generator matrix
- Decoding:
  1. Find the support of s
  2. Recover $E = S_1 \cap ... \cap S_d$, where $S_i = F_i^{-1} S$
  3. Rewrite $He^T = s$ in terms of $P = \langle E.F \rangle$
  4. Solve system, then $c = y - e$ and $m = \frac{c}{G}$

Future Research

- More attacks: adaptation of GRS attack, polynomial annulator attack
- More family of codes: simple codes, cyclic codes, QC-LRPC, DC-LRPC
- Application of codes to cryptography: GPT and LRPC cryptosystem, authentication