Ruhr University Bochum
Chair for Cryptology and IT-Security
Prof. Dr. Alexander May
Andre Esser

Kaliningrad Summerschool 2019

Day III Exercises on Subset Sum and Information Set Decoding

Exercise 1:

Give a polynomial time algorithm solving Subset Sum when $\mathbf{a}_i, \mathbf{e} \in \mathbb{Z}$, $i = 1, \ldots, n$.

Exercise 2:

You are given access to an algorithm $\mathcal{A}$ able to solve the subset sum problem in an arbitrary group $(G, \circ)$, where $\circ$ denotes the group operation. Show how to use this algorithm to solve an instance of the discrete logarithm problem $(g, \beta := g^x)$.

Exercise 3:

Consider the following algorithm for decoding a binary linear code.

Algorithm 1 Information Set Decoding

Input: parity check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$, syndrome $\mathbf{s} \in \mathbb{F}_2^{n-k}$, error weight ω
Output: $\mathbf{e} \in \mathbb{F}_2^n$ satisfying $H\mathbf{e} = \mathbf{s}$ and $\mathrm{wt}(\mathbf{e}) = \omega$

1: Randomly permute the columns of H, i.e. choose a permutation matrix $U_P \in \mathbb{F}_2^{n\times n}$ and compute $H' = HU_P$.
2: Generate identity matrix I_{n-k} on right columns of H' by adding rows, i.e. find an invertible $K \in \mathbb{F}_2^{(n-k)\times(n-k)}$ s.t. $H_s := KH' = (\tilde{H} \mid I_{n-k})$. Set $\mathbf{s}' = K\mathbf{s}$.
3: Choose $p \in \mathbb{N}$ properly (assume it given).
4: **for all** $\mathbf{e}_1 \in \mathbb{F}_2^k$ with $\mathrm{wt}(\mathbf{e}_1) = p$ **do**
5:     compute $\mathbf{e}_2 = \tilde{H}\mathbf{e}_1 + \mathbf{s}'$
6:     **if** $\mathrm{wt}(\mathbf{e}_2) = \omega - p$ **then**
7:         **return** $(\mathbf{e}_1, \mathbf{e}_2)U_P^{-1}$
8: **goto** step 1

1) Show the correctness of the algorithm.

2) Analyse the runtime / memory complexity of the algorithm. Which runtime is achieved for $k = 0.8n$ and $\omega = 0.02n$?

3) Modify the algorithm by using a Meet-in-the-Middle approach instead of bruteforcing $\mathbf{e}_1$. State the changed runtime and memory complexity.