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

Kaliningrad Summerschool 2019

Day I Exercises on the Discrete Logarithm Problem

For the following exercises we are given a generator g of a group $G = \langle g \rangle$, together with $\beta := g^x$ for $x \in \mathbb{Z}_{|G|}$, where $2^{n-1} \leq |G| < 2^n$, for some $n \in \mathbb{N}$. The goal is to compute the discrete logarithm $x = \text{dlog}_g \beta$.

Exercise 1:

Give a Meet-in-the-Middle attack on x with runtime $\tilde{\mathcal{O}}(\sqrt{x})$.

Exercise 2:

Consider the decomposition of x as $x = x_1 + x_2 \cdot 2^{\frac{n}{2}}$, where $0 \leq x_1, x_2 < 2^{\frac{n}{2}}$.

1) Given that $\text{wt}(x_1) = \text{wt}(x_2) = \alpha \cdot \frac{n}{2}$ for $\alpha \in [0, 1]$, devise an algorithm that computes x in time $\tilde{\mathcal{O}}(2^{\frac{H(\alpha)}{2}n})$. Here $\text{wt}(x) := |\{i \in \{1, \dots n\} \mid \text{bin}(x)_i = 1\}|$ denotes the Hamming weight of the binary representation of x.

2) Given that the weight does not equally split on x_1 and x_2, but still $\text{wt}(x) = \alpha n$, devise again an algorithm for computing x in $\tilde{\mathcal{O}}(2^{\frac{H(\alpha)}{2}n})$.

Exercise 3:

Given a faulty version $\tilde{x}$ of x, where x can be derived from $\tilde{x}$ by flipping αn zero bits in $\tilde{x}$ to one, $\alpha \in [0, 1]$. Additionally, we are given access to an algorithm $\mathcal{A}$ solving the low weight discrete log problem with weight parameter γ in time $T(\gamma)$. Show how to use $\mathcal{A}$ to reconstruct x from $\tilde{x}$ in time $T(\alpha)$.

Exercise 4:

Given k discrete logarithm instances in the same group: $\beta_i := g^{x_i}$, $i = 1, \dots, k$, show how to compute all x_i in time $\tilde{\mathcal{O}}(\sqrt{k \cdot |G|})$