qFALL – Exercises

Due Date: DD.MM.JJJJ
SS 2023

muster Max Mustermann 1234567

1 CTF-Like Exercises

Exercise 1
Given a falsely implemented FDH-Signature scheme based on a lattice-based PSF. The PSF returns $\mathbf{A}, \mathbf{T}$ where $\mathbf{T}$ is a trapdoor for $\mathbf{A}$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ defines the function f_a via $f_a(\mathbf{x}) := \mathbf{A} \cdot \mathbf{x}$. Show how to

1. Find a short solution for $\mathbf{Ax} = \mathbf{0}$ using only signing queries to a programmed oracle, if the storage has been completely forgotten.

2. How can you generate a second valid signature for the same arbitrarily chosen message, if the storage has been completely forgotten?

3. Find a short solution for $\mathbf{Ax} = \mathbf{0}$ using only signing queries to a programmed oracle, if the storage has been used for every message except "Hello World!".

4. How can you generate a valid signature for a arbitrarily chosen message that was not returned by the signing oracle, if the storage has been used for every message except "Hello World!"?

Hint: For 4. consider a signature scheme that accepts messages up to $s \cdot \sqrt{3m}$.

Exercise 2
Given a falsely implemented PFDH-Signature scheme based on a lattice-based PSF. The PSF returns $\mathbf{A}, \mathbf{T}$ where $\mathbf{T}$ is a trapdoor for $\mathbf{A}$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ defines the function f_a via $f_a(\mathbf{x}) := \mathbf{A} \cdot \mathbf{x}$. Show how to

1. Find a short solution for $\mathbf{Ax} = \mathbf{0}$ using only signing queries to a programmed oracle, if the randomness is only chosen from a fixed length set.

2. How can you generate a valid signature for a arbitrarily chosen message that was not returned by the signing oracle, if the randomness is only chosen from a fixed length set?

Hint: For 2. consider a signature scheme that accepts messages up to $s \cdot \sqrt{3m}$.

Exercise 3
A student has misunderstood the G-Trapdoors and directly uses Gadget-Matrices to generate LWE-Samples. Show how you can exploit the structure from the LWE samples to recompute the chosen secret, if you are given sufficiently many LWE-Samples.

2 Implementing Schemes

Exercise 4
Implement and complete the following commitment schemes[a], i.e. how do we have to set these bounds to have certain security guarantees:

1. $\text{Gen}(1^n)$: Choose $\mathbf{A}_1 \leftarrow \mathbb{Z}_q^{n\times m}$ and $\mathbf{A_2} \leftarrow \mathbb{Z}_q^{n\times k}$. Output pp $= (\mathbf{A}_1, \mathbf{A}_2)$.
2. $\text{Com}(pp, \mathbf{m})$: For $\mathbf{m} \in \mathbb{Z}_q^k$ with $\|\mathbf{m}\| \leq \beta_m$, choose $r \leftarrow D_{\mathbb{Z}^m,s}$. Compute $\mathbf{c} = \mathbf{A}_1\mathbf{r} + \mathbf{A_2}r \mod q$. Output $(\mathbf{c}, \mathbf{r})$
3. $\text{Vrfy}(pp, \mathbf{m}, \mathbf{c}, \mathbf{r}$: Check whether $\mathbf{c} = \mathbf{A}_1\mathbf{r}+\mathbf{A}_2\mathbf{m} \mod q$ and $\|m\| \leq \beta_m$ and $\|r\| \leq \beta$. If so, output 1.

[a] This task is based on HW 2.2 from the lecture PQC from the summer term 2023 in Paderborn.

Exercise 5
Implement a private key encryption scheme based on LWE.

Exercise 6
Extend the "qFALL-crypto" library.

Chose one of the following scheme ideas and make a PR that gets accepted.

- A Commitment Scheme
- IBE-Scheme based on G-Trapdoors
- Implement the Standard Model Scheme from `https://eprint.iacr.org/2011/501.pdf`
- ...

3 Non-Lattice Based

Although our library was mainly designed for lattice-based cryptography it is still very easy to implement non-lattice based cryptography.

Exercise 7
Implement one of the following schemes:

- ElGamal
- Textbook RSA
- Diffie–Hellman key exchange