Question 5

1

For a given message m, we can forge a signature under the public key $(A, \mathbf{t})$ using the following procedure:

1. Sample $\mathbf{y} \leftarrow \chi_y$
2. Compute $\mathbf{w} \leftarrow A\mathbf{y}$
3. Compute $c \leftarrow H(\mathbf{w}, \mathbf{t})$
4. Give $(A, \mathbf{w} + c\mathbf{t})$ to the module-ISIS$(k, l, q, p(x), \gamma_1 - np\tau)$ solver, which returns some $\mathbf{z}$
5. Output $\sigma = (\mathbf{w}, c, \mathbf{z})$

σ is a valid forgery because $\mathbf{z}$ as a solution to the module-ISIS$(k, l, q, p(x), \gamma_1 - np\tau)$ problem satisfies the verification conditions:

1. $\|\mathbf{z}\|_\infty \leq \gamma_1 - np\tau$
2. $A\mathbf{z} = \mathbf{w} + c\mathbf{t}$

2

The key recovery attack is as follows:

1. Sample some random message m
2. Query the signature of m, which is $(\mathbf{w}, c, \mathbf{z})$
3. Give $(A, \mathbf{w})$ to module-ISIS$(k, l, q, p(x), \gamma_1)$ solver, which returns some $\mathbf{y}$
4. Compute $\mathbf{s} = c^{-1}(\mathbf{z} - \mathbf{y})$. $\mathbf{s}$ is the secret key

This procesure works because for the queried signature to be valid, it must satisfy $\mathbf{z} = \mathbf{y} + c\mathbf{s}$, meaning that if we can recover $\mathbf{y}$, then we can recover $\mathbf{s}$. In this instance, a valid $\mathbf{y}$ is recovered using the solver on $A\mathbf{y} = \mathbf{w}$.