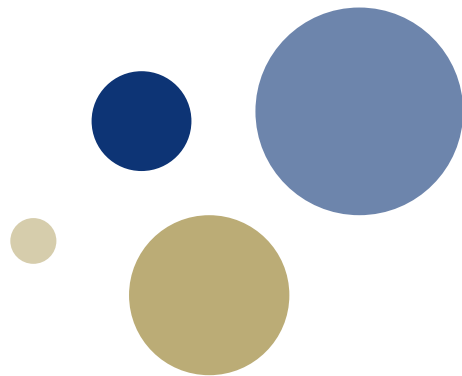




Norwegian University of  
Science and Technology



# Practical Post-Quantum Verifiable Decryption

Emil August Hovd Olaisen

# What is verifiable decryption?

- Let us suppose we have a public key encryption system with keys  $(pk, sk)$ ,  $c = \text{enc}(m, pk)$
- We want to prove that  $m = \text{dec}(c, sk)$  without revealing information about the secret key
- These schemes are particularly useful for voting schemes

# Our scheme

- The scheme is based on lattice hardness-assumptions, making it post-quantum secure
- Instead of having one pair  $(m, c)$ , we have a large number of them  $(\{m_1, m_2, \dots, m_k\}, \{c_1, c_2, \dots, c_k\})$
- The scheme verifies their correspondence together

# Our scheme

- It improves on a previous version by minimizing the size of the verifications for each message
- The setup might be cumbersome, but the work done for each message is cheaper
- Using parameters from the previous version, the proof size for each message should be about 50 times smaller

# Future work

- I am planning on looking at using techniques from the presented work on other post-quantum schemes (possibly isogenies)
- Private set intersection (PSI) allows two people to see what elements they might have in common from a set, without revealing anything else
- I know of no one who has done this post-quantum