University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 26: Post-quantum and lattice-based cryptography

April 12, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 Introduction

2 Lattice Based Crypto

1. Shortest Vector Problem (SVP)
2. Decoding (a.k.a Closest Vector or CVP)
3. Learning With Errors (LWE)

3 Learning With Errors

3.1 LWE and CVP

3.2 LWE for Key Exchange