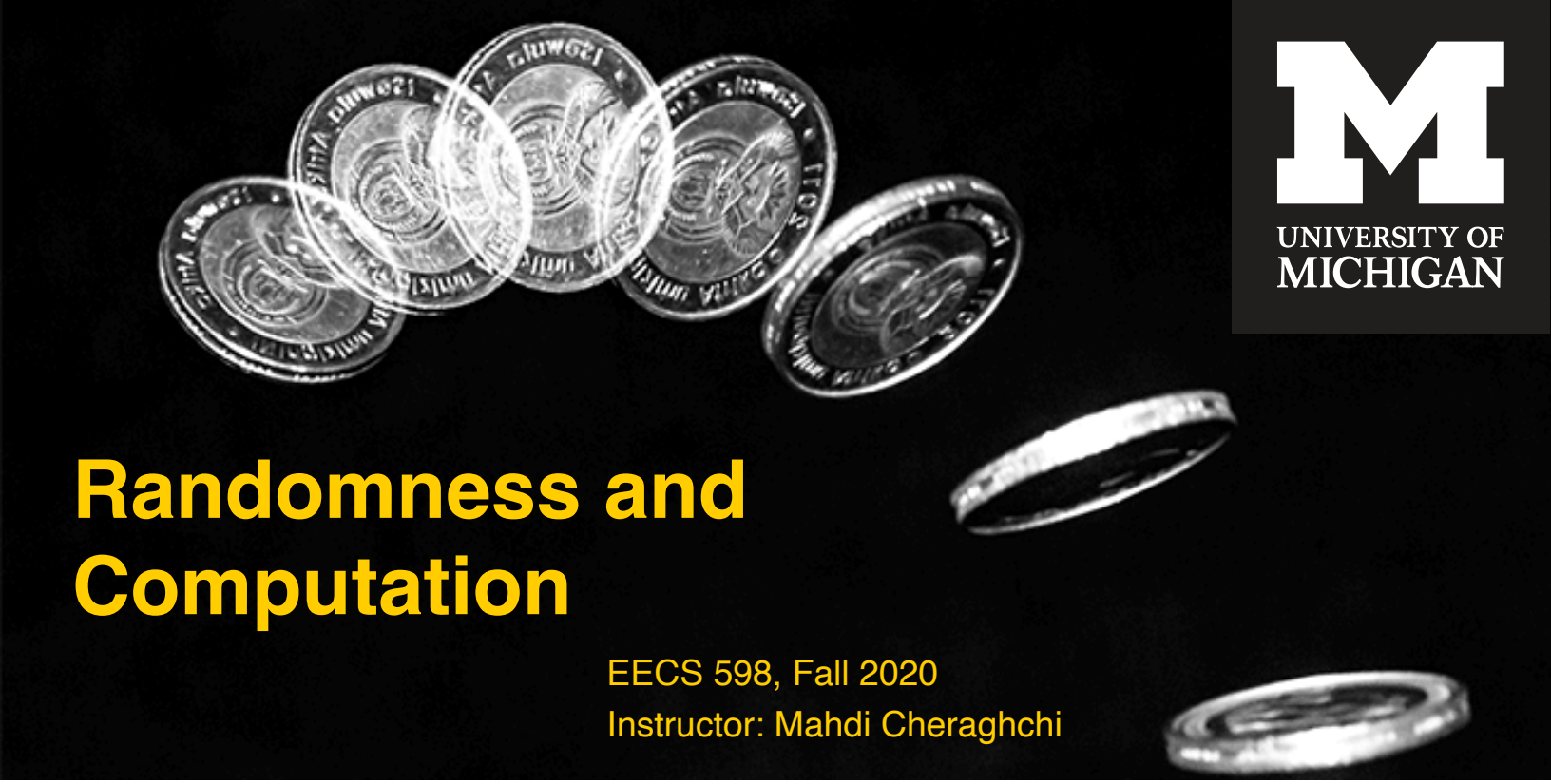

UNIVERSITY OF MICHIGAN

Randomness and Computation

EECS 598, Fall 2020

Instructor: Mahdi Cheraghchi

Along with time and memory, randomness is a fundamental resource in computation. In many cases, randomness can be used to speed up computational tasks or reduce the memory footprint, creating an entire area of *randomized algorithms*. In applications such as cryptography, randomness is a necessary aspect of computation and such system crucially rely on access to high quality random bits (for example to produce a perfectly random secret key). Moreover for such applications, the information-theoretic view of randomness is used to mathematically model uncertainty. In machine learning and computational learning, randomness and statistics are essential tools to model the computational task. The use of randomness and particularly *the probabilistic method* constitutes an important proof technique in discrete mathematics. The range of applications of randomness in computation is simply too broad to break down on a short list.

The aim of this course is to provide a mathematically rigorous exposition of the role of randomness in computation. The course will do so by showcasing examples from different application areas, such as those described above. Furthermore, time permitting, the question of simulating randomness by deterministic computation as well as extraction of randomness from weak random sources will be discussed. The precise choice of topics within the area will be flexible depending on the interests of the audience and active feedback from the students.

Prerequisites: Graduate standing, or permission of the instructor.
Advised prerequisites: EECS 203, EECS 301, EECS 376, Math 217, or equivalents.