INTRODUCTION TO QUANTUM INFORMATION

On the first day of a complexity theory course, a teacher generally introduces the complexity classes P and NP: the set of tasks that can be done efficiently on a deterministic and nondeterministic computing agent, respectively. These classes are the most important because they represent the boundary between things we can actually do on our computers in a reasonable amount of time, and things we cant.

More recently, quantum mechanics has stretched this computational boundary even further: tasks that are fundamentally impossible using the computers of today might not be for the computers of tomorrow (or at least, maybe a century from now).

The field of quantum information theory explores this question: assuming quantum mechanics is valid, what type of computational power does its view of nature give us? This is the new boundary of things we could actually do on our computers.

In this talk, I will give an abbreviated introduction to the basics of quantum information. I will discuss a few of its applications, and if time permits, I will give a brief overview of my research in the direction of quantum cryptography. Ill assume nothing more than some linear algebra and familiarity with tensor products.