Uni ct MATEMATICA E INFORMATICA

Reading Group Cryptography – prof. Dario Catalano

30h

Content of the class. We will read (more or less) recent papers in cryptography. In general, we go for papers that were recently published in top conferences in Cryptography and Theoretical Computer Science in general (such as Crypto, Eurocrypt, STOC, FOCS). The class is organized in seminars. Each seminar focuses on a single paper and lasts (roughly) two hours. The goal is to get a deep understanding of the main results of the paper. This means that the paper will be studied in all technical details. A lot of interaction is expected, and questions are always very welcome.

Required background. You should bring a solid background in cryptography and the related mathematics. This is an advanced seminar. The papers are challenging, and a proper preparation of your talk will require some eIort. Thus, you should bring a great passion for theoretical computer science. The target audience of this reading group are master students, PhD students, as well as postdocs.