Yevgeniy Dodis January 7, 2022

TEACHING STATEMENT

After arriving to NYU in January of 2001, was I faced with the exciting but challenging task of building a Cryptography Group which did not exist at the time. Big part of this task was developing new courses in cryptography in order to attract students, as well as modernizing some of the existing courses in theoretical computer science. I believe we came a long way in the past 20+ years I have been at NYU.

CRYPTOGRAPHY COURSES. I developed several state-of-the-art cryptography classes at NYU: graduate level *Introduction to Cryptography*, undergraduate level *Introduction to Cryptography*, graduate level *Advanced Cryptography*, graduate level *Research Seminar in Cryptography*, and several graduate-level special topic courses — *Exposure-Resilient Cryptography*, *Cryptography and Imperfect Randomness* and *Randomness in Cryptography*. I developed detailed lecture notes for my graduate-level classes.[1] Most notably, the evolving lecture notes for my graduate Introduction to Cryptography class [1] are repeatedly being used used at various universities as a supplemental reading for their Cryptography classes, including New Jersey Institute of Technology, University of California at Irvine and University of Bristol. On the other hand, lecture notes for my advanced cryptography classes [2, 3, 4, 5] contain some state-of-the-art research material which cannot be found anywhere, and lecturing on these advanced topics have repeatedly led to many research papers written by me and my students (examples are too numerous to list, but see one below).

I also want to point out the Spring 2013 semester, when was I on sabbatical at NEU (visiting Prof. Daniel Wichs). As part of my visit, I successfully taught the *Randomness in Cryptography* [6] class. In the course of teaching, I wrote a research paper with two graduate students at NEU (Zahra Jafargholi and Eric Miles) which got published at CRYPTO'14 [7], making this course very successful.

OTHER COURSES. In addition to my Cryptography classes, I have also taught other classes in theoretical computer science, such as Theory of Computation and Algorithms (at all levels). The algorithms class is a particularly interesting example, as this is the only required class that I had to teach, and many of the students were forced to take it without having proper background and/or motivation. I have gradually developed many tools to help students succeed. For example, carefully splitting complex problems into smaller feasible tasks, developing an extensive database of homework/exam problems, and learning how to explain things to students in a way to facilitate faster understanding. Indeed, one of the joys I get from teaching this class is frequent notes from the students saying that this was the hardest, but also the most rewarding class they have taken at NYU. Such gratitude notes never get old, and makes me really enjoy teaching.

References

[1] Yevgeniy Dodis. Lecture Notes for "Introduction to Cryptography" Class. Available at https://cs.nyu.edu/courses/spring12/CSCI-GA.3210-001/syllabus.html.

[2] Yevgeniy Dodis. Lecture Notes for "Advanced Cryptography" Class. Available at http://cs.nyu.edu/courses/fall09/G22.3220-001/syllabus.html.

[3] Yevgeniy Dodis. Lecture Notes for "Exposure-Resilient Cryptography" Class. Available at http://cs.nyu.edu/courses/spring07/G22.3033-013/syllabus.html.

[4] Yevgeniy Dodis. Lecture Notes for "Cryptography and Imperfect Randomness" Class. Available at http://cs.nyu.edu/courses/spring06/G22.3220-001/syllabus.html.

[5] Yevgeniy Dodis. Lecture Notes for "Randomness in Cryptography" Class. Available at https://cs.nyu.edu/courses/spring14/CSCI-GA.3220-001/syllabus.html.

[6] Yevgeniy Dodis. "Randomness in Cryptography" Class taught at NEU. Available at https://cs.nyu.edu/~dodis/randomness-in-crypto/index.html.

[7] Divesh Aggarwal, Yevgeniy Dodis, Zahra Jafargholi, Eric Miles and Leonid Reyzin, "Amplifying Privacy in Privacy Amplification", *Advances in Cryptology - CRYPTO*, August 2014.

[1] Unfortunately, due to new laws, several years ago NYU had to put all the course webpages behind a firewall, so that they are currently accessible only to NYU-affiliated people. I am in the process of moving important course materials to my homepage. For example, I moved my Randomness in Cryptography course already [6]. In the interim, I am happy to provide direct access to other lecture notes upon request. Indeed, several colleagues already requested some of my lectures notes for various courses.