Yevgeniy Dodis January 7, 2022

SERVICE STATEMENT

I am involved in many aspects of servicing the cryptographic community.

GLOBAL SERVICE. I served as a program co-chair for Theory of Cryptography (TCC) 2015, and about to serve as a program co-chair for CRYPTO 2022 — the most prestigious conference in cryptography. I also served as the general (or local arrangements) chair for STOC 2012, TCC 2008 and PKC 2006 conferences. I was also an Editorial Board Member for Journal of Cryptology (JoC) from 2012 to 2018, which is the premier journal in cryptography. While now I am on the Steering Committee of the Information-Theoretic Cryptography (ITC) Conference, which is the new and exciting conference focusing on the interaction on cryptography and information theory. I also served on 31 program committees since 2003 (averaging almost 2 per year) including CRYPTO/EUROCRYPT (x 13), STOC/FOCS (x 4), and TCC (x 3).

I have advised 16 Ph.D. students (including 3 female students), and 8 postdocs (1 female), who are now faculty at top academic institutions such as Cornell, Northeastern, Georgetown University, City College of NYC, University of Roschester, Chinese University of Hong Kong (CUHK), Indian Institute of Science, National University of Singapore, University of Warsaw, NYU Shanghai, or researchers in industry such as Google, IMDEA Software Institute, and Wickr. In particular, one of my former PhD students is Prof. Daniel Wichs at Northeastern University. I would be very excited to be closer to Daniel to continue our many years of fruitful collaboration. During their PhD studied, my students have won a wide array of prestigious fellowships, including NSF, NDSEG, IBM, Google and Microsoft fellowships, as well as various internal NYU award for excellence (including best thesis awards). Beyond that, I frequently collaborate with many junior researchers in the field and have often served as an informal mentor to many of them. For example, my former "de facto student" Alex Yampolskiy (officially at Yale, but most of his thesis work was joint with me) is a founder and CEO of Security Scorecard, which is an exciting company that recently reached a billion dollar valuation.

I have also done a lot of work in helping bridge communities and different sub-areas of the field of cryptography. I have over 150 coauthors (placing me among the top 7 cryptographers according to IACR crypto-db). Pre-covid times, I frequently traveled to collaborate, give talks (over 60 invited talks since 2004) and participate in cryptography events on a wide range of topics. I plan to actively continue these community building activities.

My service to the cryptographic community was explicitly listed as part of the reason why I was recently elected to become the youngest-ever Fellow of the International Association for Cryptologic Research (IACR).

LOCAL SERVICE. On a more local level to New York and New York University (NYU) in particular, for the last 20 years I co-organized a widely popular IBM/NYU/Columbia Theory Day [2], which is a semi-annual meeting aiming to bring together theoretical computer scientists in the New York area for one day of interaction and discussion. I also helped to organize the more targeted NYC Cryptography Day [3] on numerous occasions. Even more locally, 20 years ago I started our weekly NYU Cryptography seminar [1], which routinely featured state-of-the-art presentations, both external and internal. Overall, I believe that our Cryptography Group has steadily evolved into one of the top Cryptography Centers in the world: major conferences in Cryptography (CRYPTO, Eurocrypt, TCC, etc.) routinely feature multiple papers co-authored by our group members and alumni.

At the level of NYU, I served on numerous committees, such as hiring and PhD/masters admissions committee. I was also invited to participate in the NYU Scholars Lecture Series — an event introducing different areas of Arts and Science to beginning undergraduate students.

Overall, I believe serving the community is as important as research, and I plan to continue such activities.

References

[1] NYU Cryptography Seminar. Web page: http://www.cs.nyu.edu/crg/.

[2] NYU|IBM|Columbia Theory Day.
Web page: http://cs.nyu.edu/csweb/Calendar/colloquium/theory_day.html.

[3] NYC Crypto Day. Web page: https://nycryptoday.wordpress.com/.