Oxana Poburinnaya

Contact Information

- E-mail: oxanapob@bu.edu

Research Interests

I am interested in cryptography, in particular, in adaptively secure multiparty computation and deniable computation.

Education

Boston University, Boston, MA, US

Ph.D. in Computer Science **September 2013 – present**

- Advisor: Ran Canetti

Lomonosov Moscow State University, Moscow, Russia

B.Sc. **September 2008 – June 2013**

- Advisor: Nikolay Vereshagin
- Mathematics Department

Publications

Ran Canetti, Shafi Goldwasser, Oxana Poburinnaya: Adaptively Secure Two-Party Computation from Indistinguishability Obfuscation. TCC 2015.

Ran Canetti, Oxana Poburinnaya, Mariana Raykova: Optimal-Rate Non-Committing Encryption in a CRS Model. Asiacrypt 2017.

Ran Canetti, Oxana Poburinnaya, Muthuramakrishnan Venkitasubramaniam: Better Two-Round Adaptive Multiparty Computation. PKC 2017.

Ran Canetti, Oxana Poburinnaya, Muthuramakrishnan Venkitasubramaniam: Equivocating Yao: Constant-Round Adaptively Secure Multiparty Computation in the Plain Model. STOC 2017. Invited to SIAM Journal of Computing, special issue for selected papers of STOC 2017.

Internships

SRI International, summer 2015. Mentor: Mariana Raykova.

Cornell Tech, summer 2016. Mentor: Muthuramakrishnan Venkitasubramaniam.