Yilei Chen

Contact Information

857-364-7472
chenyl@bu.edu
www.chenyilei.net

Computer Science Department,
Boston University,
111 Cummington Mall, Boston MA 02215

Education

Boston University, Boston, MA — September 2012 - present

Computer Science PhD candidate.
Thesis advisors: Professor Ran Canetti and Professor Leonid Reyzin

Shanghai Jiao Tong University, Shanghai, China — September 2008 - July 2012

Bachelor of Science in Information Engineering. Member of the Honor Class.

Industrial Experience

- SRI International (Research Internship) — Menlo Park, CA, USA, June 2015 - August 2015
- Shanghai Pingyuan Consulting Co. (Co-founder) — Shanghai, China, April 2010 - February 2011

Program committee

21st International Conference on Practice and Theory of Public Key Cryptography (PKC 2018)

Publications

- *Fiat-Shamir and Correlation Intractability from Strong KDM Encryption Schemes.*
  Ran Canett, Yilei Chen, Leonid Reyzin, Ron D. Rothblum. — In submission
- *Cryptanalyses of Candidate Branching Program Obfuscators.*
  Yilei Chen, Craig Gentry, Shai Halevi. — EUROCRYPT 2017
- *Constraint-hiding Constrained PRFs for NC1 from LWE.*
  Ran Canetti, Yilei Chen. — EUROCRYPT 2017
- *Adaptive Succinct Garbled RAM, or How to delegate your database.*
  Ran Canetti, Yilei Chen, Justin Holmgren, Mariana Raykova. — TCC 2016-B
- *On the Correlation Intractability of Obfuscated Pseudorandom Functions.*
  Ran Canetti, Yilei Chen, Leonid Reyzin. — TCC 2016-A

Talks

- *Fiat-Shamir and Correlation Intractability from Strong KDM Encryption Schemes.*
  - MIT CIS seminar — Cambridge, MA, USA, December 2017
- *Cryptanalyses of Candidate Branching Program Obfuscators.*
  - Lattices and crypto meeting at ENS Lyon — Lyon, France, July 2017
  - EUROCRYPT 2017 — Paris, France, May 2017
  - Boston University security seminar — Boston, MA, USA, March 2017
- *Constraint-hiding Constrained PRFs for NC1 from LWE.*
  - Aarhus Cryptography Theory Seminar — Aarhus, Denmark, May 2017
  - EUROCRYPT 2017 — Paris, France, May 2017
  - MIT CIS seminar — Cambridge, MA, USA, March 2017
- *Adaptive Succinct Garbled RAM, or How to delegate your database.*
  - TCC 2016-B — Beijing, China, November 2016
  - DIMACS/MACS Workshop on Cryptography — Cambridge, MA, USA, June 2016
- *On the Correlation Intractability of Obfuscated Pseudorandom Functions.*
  - State Key Laboratory of Information Security — Beijing, China, October 2016
  - IST Austria — Klosterneuburg, Austria, March 2016
  - TCC 2016-A — Tel Aviv, Israel, January 2016
  - MIT CIS seminar — Cambridge, MA, USA, December 2015
  - Boston University security seminar — Boston, MA, USA, October 2015

Reference

Professor Ran Canetti (canetti@bu.edu), Department of Computer Science, Boston University, 111 Cummington Mall, Room MCS 135D, Boston, MA 02215
Professor Leonid Reyzin (reyzin@cs.bu.edu), Department of Computer Science, Boston University, 111 Cummington Mall, Room MCS 135B, Boston, MA 02215