Xin Li

Curriculum Vitae

PERSONAL DETAILS

Address	Computer Science Department, Johns Hopkins University. Baltimore, MD
Email	lixints@cs.jhu.edu
Webpage	http://cs.jhu.edu/~lixints/

RESEARCH INTERESTS

Theoretical computer science. Specifically, the use of randomness in computation, complexity theory, distributed computing, cryptography.

EDUCATION

Ph.D. in Computer Science 2005/09 - 2011/08

University of Texas at Austin, USA

Advisor: David Zuckerman.

Thesis: *Distributed Computing and Cryptography with General Weak Random Sources.*

M.S. in Computer Science 2002/09 - 2005/08

Tsinghua University, Beijing, China

B.S. in Computer Science 1998/09 - 2002/08

Tsinghua University, Beijing, China

PROFESSIONAL EXPERIENCE

Assistant Professor 2013/09 - present

Johns Hopkins University

Working on various topics in theoretical computer science.

Simons Postdoctoral Fellow 2011/09 - 2013/08

University of Washington

Worked on pseudorandomness, cryptography and problems in theoretical computer science.

Research Intern 2009/09 - 2009/12

Microsoft Research New England

Worked on applications of extractors in cryptography.

Research Assistant 2007/09 - 2011/08

University of Texas at Austin

Worked on pseudorandomness and related problems in theoretical computer science.

Supervisor: David Zuckerman.

Teaching Assistant 2005/09 - 2007/08

University of Texas at Austin

Courses: Analysis of Programs, Automata Theory, Graduate Combinatorics and Graph Theory.

PROGRAM COMMITTEE

· 19th International Workshop on Randomization and Computation (RANDOM' 2015)

REFERENCE SERVICE

- Journal Refereeing
  - · SIAM Journal on Computing (SICOMP)
  - · IEEE Transactions on Information Theory
  - · Theory of Computing (TOC)
  - · Computational Statistics
  - · Theoretical Computer Science (TCS)
  - · American Mathematical Monthly
  - · International Journal of Foundations of Computer Science (IJFCS)
  - · The Computer Journal
  - · IET Information Security (IETIS)

- Conference Refereeing
  - · ACM Symposium on Theory of Computing (STOC)
  - · IEEE Symposium on Foundations of Computer Science (FOCS)
  - · Theory of Cryptography (TCC)
  - · Innovations in Theoretical Computer Science (ITCS)
  - · International Workshop on Randomization and Computation (RANDOM)
  - · IEEE International Symposium on Information Theory (ISIT)

INVITED KEYNOTE TALK

Non-Malleable Extractors, Non-Malleable Condensers and their Applications

· 6th International Conference on Information Theoretic Security (ICITS 2012), August 2012.

INVITED TALKS

New Independent Source Extractors with Exponential Improvement

· Institute for Advanced Study, Princeton, NJ, Computer Science/Discrete Math Seminar, January 2013.
· Also at 45th Annual ACM Symposium on Theory of Computing (STOC 2013).

Privacy Amplification and Non-Malleable Extractors Via Character Sums

· Microsoft Research Redmond, Cryptography Colloquium, November 2011.
· University of Washington, Theory Seminar, October 2011.
· Also at 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011).

Improved Constructions of Three Source Extractors

· Dagstuhl Workshop, "Computational Complexity of Discrete Problems", March 2011.
· Also at 26th Annual IEEE Conference on Computational Complexity (CCC 2011).

A New Approach to Affine Extractors and Dispersers

· University of Washington, Theory Seminar, April 2012.
· Tsinghua University, Beijing, China, "China Theory Week", September 2010.
· Also at 26th Annual IEEE Conference on Computational Complexity (CCC 2011).

2-Source Extractors Under Computational Assumptions and Cryptography with Defective Randomness

· University of Texas at Austin, Theory Seminar, May 2009.
· Also at 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009).

Network Extractor Protocols

· University of Texas at Austin, Theory Seminar, September 2008.
· Also at 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2008).

CONFERENCE PRESENTATIONS

Extractors for a Constant Number of Independent Sources with Polylogarithmic Min-Entropy

· 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013).

Non-Malleable Extractors, Two-Source Extractors and Privacy Amplification

· 53rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2012).

Design Extractors, Non-Malleable Condensers and Privacy Amplification

· 44th Annual ACM Symposium on Theory of Computing (STOC 2012).

PUBLICATIONS

1 Xin Li.
Non-Malleable Condensers for Arbitrary Min-Entropy, and Almost Optimal Protocols for Privacy Amplification.
*12th IACR Theory of Cryptography Conference (***TCC 2015***).*

2 Kai-Min Chung, Xin Li and Xiaodi Wu.
Multi-Source Randomness Extractors Against Quantum Side Information, and their Applications. *Electronic Colloquium on Computational Complexity (***ECCC 2014***).*

3 Yevgeniy Dodis, Xin Li, Trevor D. Wooley and David Zuckerman.
Privacy Amplification and Non-Malleable Extractors Via Character Sums.
*SIAM Journal on Computing (***SICOMP 2014***). Preliminary version in 52nd Annual IEEE Symposium on Foundations of Computer Science (***FOCS 2011***).*

4 Xin Li.
Extractors for a Constant Number of Independent Sources with Polylogarithmic Min-Entropy.
*54th Annual IEEE Symposium on Foundations of Computer Science (***FOCS 2013***).*
Invited to SICOMP Special Issue for FOCS 2013.

5 Yuval Ishai, Eyal Kushilevitz, Xin Li, Rafail Ostrovsky, Manoj Prabhakaran, Amit Sahai and David Zuckerman.
Robust Pseudorandom Generators.
*40th International Colloquium on Automata, Languages and Programming (***ICALP 2013***).*

6 Xin Li.
New Independent Source Extractors with Exponential Improvement.
*45th Annual ACM Symposium on Theory of Computing (***STOC 2013***).*

7 Xin Li.
Non-Malleable Extractors, Two-Source Extractors and Privacy Amplification.
*53rd Annual IEEE Symposium on Foundations of Computer Science (***FOCS 2012***).*

8 Xin Li.
Design Extractors, Non-Malleable Condensers and Privacy Amplification.
*44th Annual ACM Symposium on Theory of Computing (***STOC 2012***).*

9 Xin Li.
Improved Constructions of Three Source Extractors.
*26th Annual IEEE Conference on Computational Complexity (***CCC 2011***).*

10 Xin Li.
A New Approach to Affine Extractors and Dispersers.
*26th Annual IEEE Conference on Computational Complexity (***CCC 2011***).*

11 Yael Tauman Kalai, Xin Li and Anup Rao.
2-Source Extractors Under Computational Assumptions and Cryptography with Defective Randomness.
*50th Annual IEEE Symposium on Foundations of Computer Science (***FOCS 2009***).*

12 Yael Tauman Kalai, Xin Li, Anup Rao and David Zuckerman.
Network Extractor Protocols.
*49th Annual IEEE Symposium on Foundations of Computer Science (***FOCS 2008***).*

13 Runyao Duan, Yuan Feng, Xin Li and Mingsheng Ying.
Multiple-copy entanglement transformation and entanglement catalysis.
*Physical Review A 2005 (***PRA 2005***).*

14 Runyao Duan, Yuan Feng, Xin Li and Mingsheng Ying.
Trade-off between multiple-copy transformation and entanglement catalysis.
*Physical Review A 2005 (***PRA 2005***).*

15 Xin Li, Luo Sun, Linmi Tao, Guangyou Xu and Ying Jia.
A Speaker Tracking Algorithm Based on Audio and Visual Information Fusion Using Particle Filter.
*1st International Conference on Image Analysis and Recognition (***ICIAR 2004***).*