Guang Yang

Curriculum Vitae

Institute for Interdisciplinary Information Sciences (IIIS)
FIT 4-609, Tsinghua University
10084, Beijing, P. R. China
+86 138 1043 2282
guang.research@gmail.com
iiis.tsinghua.edu.cn/guangyang/

Research Areas

Foundations of Cryptography: Constructions of cryptographic primitives (OWF, PRG, etc.) and cryptosystems (PKE, MAC, digital signature, etc.). Leakage-ressilient circuits. Zero-knowledge PCP protocols.

Randomness and Derandomization: Randomness extraction, seedless extractors, multi-source extractors. Implementation of randomness extractors. Pseudorandom generators, expander graphs, dispersers.

Streaming Computation: Computational complexity across streaming classes (with various settings), lower bounds and reductions. Multi-Stream model, efficient algorithms with tiny memory and almost constant many passes over read/write streams. Techniques for streaming algorithms, e.g. separating the space complexity of streaming algorithms from worst-case partition communication complexity.

Learning Theory: Ensemble methods. Metric embedding. The power of geometric properties in learning tasks, e.g. learning low-distortion concepts.

Education

2010 — **PhD** in Computer Science, *Tsinghua University*, Beijing.
Institute for Interdisciplinary Information Sciences (IIIS)

Thesis title *Cryptography and Randomness Extraction in the Multi-Stream Model*

Advisor Periklis A. Papakonstantinou

2006 – 2010 — **B.Eng.** in Computer Science, *Tsinghua University*, Beijing.

Research Papers

- Making the Best of a Leaky Situation: Zero-Knowledge PCPs from Leakage-Resilient Circuits. (with *Yuval Ishai and Mor Weiss*). **TCC 2016**.
- Incompressible Functions, Relative-Error Extractors, and the Power of Nondeterministic Reductions. (with *Benny Applebaum, Sergei Artemenko, and Ronen Shaltiel*). **CCC 2015**.
- Cryptography with Streaming Algorithms. (with *Periklis A. Papakonstantinou*). **CRYPTO 2014**.
- A Remark on One-Wayness versus Pseudorandomness. (with *Periklis A. Papakonstantinou*). **COCOON 2012**.
- Reversing Longest Previous Factor Tables is Hard. (with *Jing He and Hongyu Liang*). **WADS 2011**.

Talks and Presentations

Nov 2015 Cryptography and Randomness Extraction with Streaming Algorithms.
Bell Labs. Host: Vlad Kolesnikov.

Nov 2015 Streaming Computation and Lower Bounds.
Business School, Rutgers University.

Nov 2015 Streaming Computation – models, algorithms, and lower bounds.
Invited mini-course at Rutgers University. Host: Nabil Adams.

Oct 2014 Extract Randomness from Big Data Streams – from Theory to Practice.
Theory of Cryptography workshop, Tsinghua University, Beijing.

Sep 2014 Randomness and Pseudorandomness in Data Streams.
The 8th China Theory Week, Tsinghua University, Beijing.

Aug 2014 Cryptography with Streaming Algorithms.
CRYPTO 2014.

Aug 2014 Streaming Randomness Extraction.
Rump Session of CRYPTO 2014.

Mar 2014 Streaming Cryptography – lower bounds.
Center for the Theory of Interactive Computation (CTIC), Aarhus University, Denmark. Host: Peter Bro Miltersen.

Oct 2013 Streaming Cryptography.
GTACS seminar, Bar Ilan University, Israel. Host: Benny Applebaum.

Jun 2013 Streaming Cryptography.
SIGMA seminar at ICT, Chinese Academy of Sciences (CAS). Host: Xiaoming Sun.

Aug 2012 Streaming Cryptography.
Rump Session of CRYPTO 2012.

Jul 2012 Streaming Cryptography – preview of possibilities.
ITCSC, Chinese University of Hong Kong (CUHK), Host: Andrej Bogdanov.

Aug 2011 Reversing Longest Previous Tables is Hard.
WADS 2011, New York University.

Selected Awards

- National Scholarship for Graduate Students, 2014
- Recognition Award of Institute for Interdisciplinary Information Sciences, 2011
- Gold Medal in China Mathematical Olympiad, 2006

Research Experience

Fall, 2013 Technion – Israel Institute of Technology (hosted by Yuval Ishai and Eyal Kushilevitz).

Fall, 2013 Tel-Aviv University (hosted by Benny Applebaum).

Summer, 2012 The Chinese University of Hong Kong (visiting the Institute for Theoretical Computer Science and Communications).

Fall, 2009 MIT (hosted by Silvio Micali).

Teaching Experience

Courses

Fall, 2014 TA for *Algorithms and Models for Big Data*. Instructor: Periklis A. Papakonstantinou.

Spring, 2013 TA for *Machine Learning and Pattern Recognition*. Instructor: Jia Xu.

Fall, 2012 TA for *Introduction to Computer Science*. Instructor: Andrew Chi-Chih Yao.

Spring, 2012 TA for *Mathematics for Computer Science*. Instructor: Andrew Chi-Chih Yao.

Fall, 2011 TA for *Fundamental Ideas in Theoretical Computer Science*. Instructor: John Steinberger.

Spring, 2011 TA for *Mathematics for Computer Science*. Instructor: Andrew Chi-Chih Yao.

Spring, 2011 TA for *Theoretical Computer Science (II)*. Instructor: Xiaoming Sun.

Fall, 2010 TA for *Theoretical Computer Science (II)*. Instructor: Kevin Matulef

Supervised Students

Nov 2014 – Aug 2015 Zhengyang Song. *The implementation of randomness extractors*, undergraduate research project.