

Periklis A. Papakonstantinou

Dept. of Management Science and Information Systems
Rutgers Business School
94 Rockafeller Road, Rm# 229
Piscataway, NJ 08854
papakons@business.rutgers.edu
<http://papakons.business.rutgers.edu>
848-445-9225

Research Interests Computing over Big Data-streams, Machine Learning
Foundations of Computer Science, Cryptography

Employment **Rutgers University** 9.2015 – current

- Assistant Professor at MSIS, Rutgers Business School
(to be promoted to Associate Professor with tenure from 7.2018)

Tsinghua University 3.2010 – 8.2015

- Assistant Professor & PhD Supervisor at IIIS
- Head of the Randomness in Computation and Cryptographic Complexity laboratory

Other Affiliations **Department of Computer Science, Rutgers Univ.** 3.2017 – current
Associate Member of the Graduate Program (courtesy appointment)

DIMACS 4.2016 – current
Member

Academic Visits **UC Berkeley, Simons Institute** 1.2014 – 3.2014
Visiting Researcher

University of Toronto, Dept. Computer Science 6.2012 – 8.2012
Visiting Professor

Education **University of Toronto** 9.2004 – 2.2010
PhD in Computer Science
Thesis: Constructions, lower bounds, and new directions in Cryptography and Computational Complexity
Advisor: Charles W. Rackoff

University of Toronto MSc in Mathematics Thesis: Growth in Families of Finite Groups Advisor: Gábor Pete	9.2006 – 5.2008
University of Toronto MSc in Computer Science Thesis: Hierarchies and Complexity Results for Priority Algorithms Advisor: Charles W. Rackoff	9.2002 – 1.2004
University of Patras Diploma (BEng & MEng program) in Computer Eng. and Science <i>Summa cum laude</i> (rank: 1st)	9.1996 – 8.2001

Publications

Remark: in all papers the author order is alphabetical

- **Lower bounds, Randomness, Derandomization**

1. *Depth-reduction for composites*
with Shiteng Chen
Foundations of Computer Science (FOCS), 2016
Invited to the SIAM Journal of Computing (SICOMP), 2017
(invitation given to the best papers at FOCS)
2. *Correlation lower bounds from correlation upper bounds*
with Shiteng Chen
Information Processing Letters (IPL), 2016
3. *Pseudorandomness for linear length branching programs & stack machines*
with Andrej Bogdanov and Andrew Wan
RANDOM, 2012
4. *Pseudorandomness for read-once formulas*
with Andrej Bogdanov and Andrew Wan
Foundations of Computer Science (FOCS), 2011
5. *How strong is Nisan's pseudo-random generator?*
with Matei David and Anastasios Sidiropoulos
Information Processing Letters (IPL), 2011
6. *Computationally Limited Randomness*
with Matei David, Phuong Nguyen, and Anastasios Sidiropoulos
Innovations in Theoretical Computer Science (ITCS), 2011
7. *Tradeoff lower bounds for Stack Machines*
with Matei David
Conference in Computational Complexity (CCC), 2010
journal version: Computational Complexity

- **Foundations and Cryptography over Big Data**

8. *True Randomness from Big Data*
with David Woodruff and Guang Yang
Sci.Rep. (Nature's Scientific Reports) , 2016
9. *Cryptography with streaming algorithms*
with Guang Yang
CRYPTO, 2014
10. *Limits on the stretch of non-adaptive constructions of pseudo-random generators*
with Josh Bronson and Ali Juma
Theory of Cryptography Conference (TCC), 2011
11. *On the impossibility of basing Identity Based Encryption on trap-door permutations*
with Dan Boneh, Yevgeniy Vahlis, Charles W. Rackoff, and Brent Waters
Foundations of Computer Science (FOCS), 2008
12. *A remark on one-wayness versus pseudo-randomness*
with Guang Yang
Computing and Combinatorics Conference (COCOON), 2012

- **SAT-solving and SAT algorithms**

13. *Local Search for Hard SAT Formulas: the Strength of the Polynomial Law*
with Sixue Liu
AAAI, 2016
14. *Width-parameterized SAT: time-space tradeoffs*
with Eric Allender, Shiteng Chen, Tiancheng Lou, and Bangsheng Tang
Theory of Computing, 2014
15. *A note on width-parameterized SAT - an exact machine characterization*
Information Processing Letters (IPL), 2009
16. *Complexity and algorithms for well-structured k -SAT instances*
with Kostantinos Georgiou
Theory and Applications of Satisfiability Testing - SAT, 2008

- **Space-bounded communication complexity**

17. *Overlays and Limited Memory Modes*
with Dominik Scheder, and Hao Song
Conference in Computational Complexity (CCC), 2014
18. *Space-bounded Communication Complexity*
with Joshua Brody, Shiteng Chen, Hao Song, and Xiaoming Sun
Innovations in Theoretical Computer Science (ITCS), 2013

- **Machine Learning over Big Data**

19. *On the Power and Limits of Distance-Based Learning*
with Guang Yang and Jia Xu
ICML, 2016

20. *Bagging-by-design (Bagging is Sub-Optimal)*
with Jia Xu, and Zhu Cao
AAAI, 2014

- **Theory of simple algorithms**

21. *On the structure of optimal greedy computation (for Job Scheduling)*
Mathematical Foundations of Computer Science (MFCS), 2009

22. *Characterizing sets of jobs that admit optimal greedy-like alg.*
with Charles W. Rackoff
Journal of Scheduling, 2010

23. *Hierarchies for classes of priority algorithms for Job Scheduling*
Theoretical Computer Science, 2006

- **Miscellanea**

24. *On the Complexity of Constructing Golomb Rulers*
with Christophe Meyer
Discrete Applied Mathematics, 2009

25. *Bounded and Ordered Satisfiability: Connecting Recognition with Lambek-style Calculi to Classical Satisfiability Testing*
with Michail Flouris, Lap Chi Lau, Tsuyoshi Morioka, and Gerald Penn
Mathematics of Language, 2003

*Research
Grants*

- **National Science Foundation of China** 1.2011 – 12.2014
800,000RMB (\$130,000 USD)
Principal Investigator, *Streaming Cryptography*
- **Beijing Government Fund for Excellence** 1.2013 – 12.2015
150,000RMB (\$25,000 USD)
Personal Award
- **National Science Foundation of China** 1.2011 – 12.2013
2,600,000RMB (\$428,000 USD)
Key Member, Principal Investigator: Andrew Yao, *Computational and Communication Complexity and Quantum Computation*
- **National Science Foundation of China** 1.2013 – 12.2015
660,000RMB (\$107,000 USD)
Key Member, Principal Investigator: Iddo Tzameret, *Logic, Cognition, and Proof Systems*

PhD

Supervision

Officially supervised PhD students (graduated):

- Shiteng Chen (degree conferred: 6.2016)
now Assistant Professor at the Chinese Academy of Sciences
– Institute of Software, CAS
- Guang Yang (degree conferred: 1.2016)
now Assistant Professor at the Chinese Academy of Sciences
– Institute of Computing Technology, CAS
- Hao Song (degree conferred: 6.2014)
now at pony.ai; previously Engineer at Facebook, Menlo Park,
California
- Bangsheng Tang (degree conferred: 6.2013)
now researcher at Facebook, Menlo Park, California
former research director at Hulu, Beijing office

MSc &

Undergraduate

Theses

Supervision

MSc thesis advisor:

- Sixue Liu (degree conferred: 6.2016)
now PhD student at Princeton
- Silvio Frischknecht (degree conferred: 10.2012)
Silvio was an ETH-Zurich student (Swiss Federal Institute of
Technology) who did his thesis at Tsinghua (officially co-
supervised with Roger Wattenhofer)

Undergraduate thesis advisor for the following Tsinghua students:

- Yuping Luo (degree conferred: 6.2017)
now PhD student at Princeton
- Lei Zhixiang (degree conferred: 6.2016)
now PhD student at Harvard
- Yuanzhi Li (degree conferred: 6.2014)
now PhD student at Princeton
- Xin Yang (degree conferred: 6.2014)
now PhD student at the University of Washington
- Mao Jieming (degree conferred: 6.2013)
now PhD student at Princeton

Other student mentorship

- REU program at DIMACS:
 - 6 students from Charles University, Prague (5/2017 – current)
 - Brad Bentz, intern from Brown University (5/2016 – 7/2016)
- Capstone projects: 5 capstone projects at RBS
1 capstone project at Rutgers CS

*Editor,
Service &
Administration*

- Associate Editor for Discrete Applied Mathematics
- I served in the program committees of
 - 26th & 27th WWW
 - 21st COCOON
 - 13th conference on Applied Crypto. & Network Security
 - 41st International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2015)
 - TAMC 2013
 - Annual Privacy Forum, Closing the Loop from Research to Policy, 2012
 - 8th International Conference on Algorithmic Aspects of Information and Management (FAW/AAIM 2012)
- I served as a program committee chair for the following events:
 - *Trends in Theoretical Cryptography 2011* 1.2011
organizer - program chair
 - *China Theory Week 2010* 9.2010
program chair
- Comp. Complexity work-package leader 4.2010 – 8.2015
 - *Sino-Danish Center for the Theory of Interactive Computation*

*Scholarships
Honors, &
Awards*

- **Beijing Higher Education Young Talent Award** 9.2013
Education Council of Beijing
- **Fellowship from the Dept. of Comp. Science** 9.2002 – 1.2010
University of Toronto
- **Award from the State Scholarships Foundation (of Greece)**
“due to overall outstanding academic performance for the undergraduate studies from 1996 – 2001”, for being the rank-first student in his department
- **EU award of excellence in engineering studies** 12.2002
awarded by the Technical Chamber of Greece
- **First Award from the Skouras Foundation** 5.2002
for the highest graded graduate in 2001 (approximately 1700 grads Schools: Engineering, Natural Sci., Medicine, Philosophy)
- **Highest graded student at the School of Engineering** 11.2001
University of Patras (valedictorian)
- **Best poster award** 6.2001
Periklis A. Papakonstantinou and Anastasios Sidiropoulos, *Evolution Algorithms in chaotic time-series*, 14th Conf.on Nonlinear Dynamics: Chaos and Complexity
- **1st place in the annual national (Greece/Cyprus) collegiate programming contest** 5.1998

Teaching

I designed and instructed for the following courses:

- **Information Security** (undergraduate)
Rutgers University, Spring 2017
- **Applications of Machine Learning on Big Data** (PhD)
Rutgers University, Spring 2016
- **Business Data Management (Databases)** (MBA & MB-IT)
Rutgers University, Spring 2016, Spring 2017
- **Data Privacy** (PhD)
Rutgers University, Fall 2015, Fall 2016
- **Cryptography** (undergraduate)
Tsinghua University, Spring 2015
- **Algorithms and Models for Big Data** (undergraduate)
Tsinghua University, Fall 2014
- **Circuit Complexity Now and Then** (graduate)
Tsinghua University, 4.2014 – 6.2014
- **Algorithm Design and Analysis** (undergraduate)
Tsinghua University, Fall 2013
- **Contemporary topics in the Foundations of Cryptography**
(graduate) Tsinghua University, Spring 2013
- **Representations and Algorithms in Groups** (undergraduate)
Tsinghua University, Fall 2012
- **Randomness in computation and Derandomization** (grad.)
co-taught with Jian Li, Tsinghua University, Spring 2012
- **Propositional Proof Complexity** (graduate)
co-taught with Iddo Tzameret, Tsinghua University, Fall 2011
- **Advanced Algorithms** (undergraduate)
Tsinghua University, Fall 2011 and Spring 2011
- **Graduate Computational Complexity** (graduate)
Tsinghua University, Fall 2010
- **CSC – 310 Information Theory** (undergraduate)
University of Toronto, Fall 2009
- **CSE – 3101 Design and Analysis of Algorithms** (undergrad.)
York University, Canada
Summer 2008, Fall 2005, Summer 2004
- **ECE – 190 Discrete Mathematics** (undergraduate)
University of Toronto, Fall 2006

*Invited
Talks*

- **Depth Reduction with Composites**
Columbia University, Dept. of Computer Science (DCS) 4.2016
Princeton University, DCS 3.2016
- **Bagging in the Real World**
4th (Rutgers) Applied Probability Conference 11.2015
Chinese Academy of Sciences, Inst. of Software 4.2015
- **True Randomness from Big Data**
Rutgers University, Theory Group Seminar 11.2015
Chinese Academy of Science, Inst. of Comp. Tech. 5.2015
- **Cryptography over Big Data**
Workshop on Theoretical Aspects of Big Data 7.2013
Imperial College, Dept. of Computing 7.2012
École Normale Supérieure, Paris 7.2012
- **Pseudorandomness: when order matters**
Workshop on Algebraic Complexity Theory 3.2013
- **Space-bounded Communication Complexity**
Princeton University, DCS 7.2012
- **Width-parameterized SAT: time-space tradeoffs**
University of British Columbia, DCS 8.2012
Laboratoire d'Informatique (at Paris 11) 7.2012
Chinese Academy of Sciences, Inst. of Software 3.2012
- **New questions in pseudo-randomness for answering old problems**
Microsoft Research Asia (at SHJT) 5.2012
Workshop on Synergies in Lower Bounds 6.2011
ITCSC at CUHK 9.2011
- **The Limits of Decisional Diffie-Hellman and Trapdoor Permutations**
Mini-workshop on the Theory of Computing at CUHK 8.2010
- **Understanding the structure of optimal greedy computation**
University of Toronto, Theory Seminar 7.2012
- **On the impossibility of basing Identity Based Encryption on trapdoor permutations**
Centre for Applied Cryptographic Research, U Waterloo 12.2009
- **New directions in derandomization**
Cheriton School of Computer Science, U Waterloo 1.2009

*Selected
other
Work
Experience*

- Research associate 2.2004 – 8.2004
Architectures of peer-to-peer systems
Technical University of Crete, Lab Director: Manolis Koubarakis
- Research Assistant for EXAPSIS (EU Project) 5.2000 – 6.2001
Active Disk Technologies, Research director: Peter Triantaffilou

- *Cooperative Loans Management System* 5.2000 – 9.2000
Distributed system for the Agricultural Bank of Greece: project planning and management, design, implementation of the distributed protocols and database system (First Informatics S.A.)

Licensed Electronics Engineer with the Tech. Chamber of Greece
3.2004 –

Languages

Fluent in English and Greek

Very good knowledge of French
(Académie Française d' Athènes: DELF A₁ - A₄)

Basic oral (Mandarin) Chinese