David Xiao

dxiao@liafa.univ-paris-diderot.fr
LIAFA
Université Paris Diderot - Paris 7
Case 7014
75205 Paris Cedex 13
France

Research interests:

Cryptography and Privacy, Complexity, Game theory, Learning theory

Employment

CNRS, LIAFA, Université Paris 7 (Oct. 2011 – present)

Research Scientist (CR2) in Algorithms and Complexity Group

LRI Université Paris-Sud and LIAFA, Université Paris 7 (Sep. 2009 – Oct 2011):

Post-doc in Algorithms and Complexity group

Education:

Graduate:

- Princeton University, Princeton, NJ. **Ph D Computer Science**, September 2009.
  - Thesis: *New Perspectives on the Complexity of Computational Learning, and Other Problems in Theoretical Computer Science.*
  - Advisors: Boaz Barak and Avi Wigderson (IAS)
- Université Pierre et Marie Curie Paris VI, Paris, France: **Maîtrise Pure Mathematics**, June 2004 *mention très bien* (highest honors)
- Harvard University, Cambridge, MA: **SM Computer Science**, June 2003

Undergraduate:

- Harvard University, Cambridge, MA: **AB Computer Science**, June 2003 *summa cum laude*.
  - Thesis: *The Evolution of Expander Graphs.* Awarded Hoopes Prize.
  - Advisor: Salil Vadhan

Conference and Journal Publications:

- *Bell tests and applications to communication and information complexity*
  I. Kerenidis, S. Laplante, V. Lerays, J. Roland, and D. Xiao
  QIP 2013

- *Languages with efficient Zero Knowledge PCPs are in SZK*
  M. Mahmoody and D. Xiao
  TCC 2013
- *Is privacy compatible with truthfulness?*
  D. Xiao
  ITCS 2013
- *Lower bounds on information complexity via zero-communication protocols and applications*
  I. Kerenidis, S. Laplante, V. Lerays, J. Roland, and D. Xiao
  FOCS 2012
- *Round-optimal black-box statistically binding selective-opening secure commitments*
  D. Xiao
  Africacrypt 2012
- *Improved bounds for the randomized decision tree complexity of recursive majority*
  F. Magniez, A. Nayak, M. Santha, and D. Xiao.
  ICALP 2011
- *(Nearly) round-optimal black-box constructions of commitments secure against selective opening attacks*
  D. Xiao.
  TCC 2011
- *On the round complexity of zero-knowledge proofs from one-way permutations*
  S. Gordon, H. Wee, A. Yerukhimovich, and D. Xiao.
  Latincrypt 2010
- *Learning to create is as hard as learning to appreciate.*
  D. Xiao.
  COLT 2010
- *On the power of randomized reductions and the checkability of SAT.*
  M. Mahmoody and D. Xiao.
  CCC 2010
- *A new sampling protocol and applications to basing cryptographic primitives on NP.*
  I. Haitner, M. Mahmoody, and D. Xiao.
  CCC 2010
- *On basing ZK ≠ BPP on the hardness of PAC learning.*
  D. Xiao.
  CCC 2009
- *On basing lower-bounds for learning on worst-case assumptions.*
  B. Applebaum, B. Barak, and D. Xiao.
  FOCS 2008
- *Path quality monitoring in the presence of adversaries.*
  S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford.
  SIGMETRICS 2008.
- *Protocols and lower bounds for failure localization on the Internet.*

B. Barak, S. Goldberg, and D. Xiao.
EUROCRYPT 2008.

- *Derandomizing the Ahlswede-Winter matrix-valued Chernoff Bound via pessimistic estimators and applications.*
  A. Wigderson and D. Xiao.
  Theory of Computing, Vol. 4 No. 3 (2008)
- *A randomness-efficient sampler for matrix-valued functions and applications.*
  A. Wigderson and D. Xiao.
  FOCS 2005
- *Estimating and comparing entropy across written natural languages using PPM compression.*
  F. Behr, V. Fossum, M. Mitzenmacher, and D. Xiao.
  DCC 2003

Other Publications:

- *Pseudo-aléa: objets et generation*
  D. Xiao
  Journées annuelles de la Société Mathématiques de France, 2011
- *Comment se mettre d'accord sur un rendez-vous?*
  D. Xiao
  La Recherche, 2011

Academic Awards, Fellowships, and Distinctions:

NDSEG Department of Defense Graduate Fellowship

NSF Graduate Fellowship

Francis Upton Graduate Fellowship (Princeton University)

Hoopes Prize for Outstanding Undergraduate Thesis (Harvard University)

Phi Beta Kappa (Alpha Iota Chapter)

CRA Outstanding Undergraduate Award Honorable Mention

John Harvard Scholarship Recipient (all years at Harvard)

Detur Book Prize Award from Harvard College

National Merit Scholarship Recipient

Massachusetts Telecommunications Council Technical Achievement Award

Teaching Experience:

Fall 2012: **Randomness in Complexity:** MPRI course 2.11.2

Fall 2011: **Randomness in Complexity:** MPRI course 2.11.2

Spring 2011: **Pseudorandomness**: invited mini-course, Journées ALEA 2011

Spring 2006: **The Computational Universe:** Princeton University COS 116

Fall 2005: **Cryptography:** Princeton University COS 433

Invited talks

DIMACS Workshop on Recent Work on Differential Privacy across Computer Science. DIMACS, 2012.

Tsinghua-MIT-CUHK Research Center Workshop on Theoretical Computer Science. Chinese University of Hong Kong, China. 2012

Workshop on Synergies in Lower Bounds. Aarhus University, Denmark. 2011.

Trends in Theoretical Cryptography, IIIS Tsinghua University, China. 2011.

Other Research Experience:

Microsoft Research New England (Summer 2012):

Visiting scientist

Microsoft Research Asia (Summer 2010):

Visiting scientist

Tsinghua University (Summer 2008):

Visiting student at the Institute for Theoretical Computer Science

IBM Research Yorktown Heights (Summer 2007)**:**

Summer intern in quantum computation group

Languages

English (native), Mandarin Chinese (fluent), French (fluent), Hebrew (elementary)