

David Xiao
dxiao@lri.fr
Bat. 490
Université Paris-Sud
91405, Orsay
France

Research interests:

Complexity, Cryptography, Learning theory, Derandomization, Security

Education:

Graduate:

Princeton University, Princeton, NJ. **Ph D Computer Science**, graduated September 2009

Université Pierre et Marie Curie Paris VI, Paris, France: **Maîtrise Pure**

Mathematics, graduated June 2004 *mention très bien* (highest honors)

Harvard University, Cambridge, MA: **SM Computer Science**, graduated June 2003

Undergraduate:

Harvard University, Cambridge, MA: **AB Computer Science**, graduated June 2003
summa cum laude.

Publications:

New Perspectives on the Complexity of Computational Learning, and Other Problems in Theoretical Computer Science. D. Xiao. Ph. D thesis, Princeton University, 2009.

On basing $ZK \neq BPP$ 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

The Evolution of Expander Graphs. D. Xiao. Senior Thesis, Harvard 2003. Awarded Hoopes Prize.

Estimating and Comparing Entropy Across Written Natural Languages Using PPM Compression. F. Behr, V. Fossum, M. Mitzenmacher, D. Xiao DCC 2003: 416

Other Research Experience:

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

Teaching Experience:

The Computational Universe: Princeton University COS 116, Spring 2006

Introduction to computer science for non-majors.

Developed course material

Instructed weekly lab sessions

Cryptography: Princeton University COS 433, Fall 2005

Introduction to theoretical cryptography

Instructed weekly recitations

Academic Awards, Scholarships, and Fellowships:

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

Work Experience:

Research Intern: IBM Research, Hawthorne, NY (Summer 2003)

Researched applying autonomic policies to massive distributed storage networks

Developed policy engine for Storage Tank (a.k.a. SAN FS) filesystem

Introduced the idea of market mechanisms into filesystem allocation in Storage Tank

Software Development Engineer Intern: Microsoft, Redmond, WA (Summer 2002)

Research into audio watermarking algorithms and applicability of image watermarking techniques to audio

Signal processing programming in C++ and Matlab

Implementation of audio watermarking DirectX Media Object

Software Engineer Intern: Lycos, Inc., Waltham, MA (Summer – Winter 2000)

Rewrite of internal web server log analysis tool

Distributed programming using Jini and Javaspace

Database programming using JDBC and MS SQL Server

Software Research Intern: Lycos, Inc., Waltham, MA (Summer 1999)

Research into effectiveness of PHP and JSP as scripting languages

Reverse-engineering of PHP module API

Development of native interface between Lycos' search engine and the PHP and JSP environments

Languages

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