Michael J. Freedman

353 Serra Mall, Room 288
Stanford, CA 94305-9025
(650) 723-1863

http://www.michaelfreedman.org/
mfreed@scs.stanford.edu
Citizenship: US

Education

New York University .... New York, NY

Ph.D. Candidate in Computer Science .... Expected May 2007
Thesis title: *Democratizing Content Distribution*
Visiting **Stanford University**, September 2005–May 2007
Advisor: David Mazières ; GPA: 4.0/4.0

M.S. in Computer Science .... May 2005
Advisor: David Mazières ; GPA: 4.0/4.0

Massachusetts Institute of Technology .... Cambridge, MA

M.Eng. in Electrical Engineering and Computer Science .... June 2002
Thesis title: *A Peer-to-Peer Anonymizing Network Layer*
Advisor: Robert Morris ; GPA: 5.0/5.0

S.B. in Computer Science, Minor in Political Science .... June 2001
Thesis title: *An Anonymous Communications Channel for the Free Haven Project*
Advisor: Ron Rivest ; GPA: 4.9/5.0

Interests

Distributed systems, security, networking, and cryptography

Research

2002–present

Cooperative content distribution. Conceived and led the Coral Project. Designed and built an Internet-scale, self-organizing web-content distribution network: CoralCDN [12] uses a network of cooperating DNS redirectors and HTTP proxies, backed by a decentralized indexing infrastructure [19], to allow oblivious clients to transparently download content from nearby servers, while avoiding distant or heavily-loaded ones. CoralCDN has been in production use on 300 servers since March 2004, currently receiving about 25 million HTTP requests from over 1 million clients per day, serving several terabytes of data. `http://coralcdn.org/`

With a focus on settings with mutually-distrustful clients, Shark [7] provides a distributed file system that improves scalability and performance through cooperative reads, using Coral's indexing layer to locate files. Yet Shark preserves traditional semantics, manageability, and security. Other research provides integrity guarantees for large files encoded with rateless erasure codes, via a homomorphic hash function that can verify downloaded blocks on-the-fly [11].

Ongoing focus on untrusted settings for CDNs (with C. Aperjis, R. Johari, and D. Mazières), devising incentive-compatible mechanisms that cause nodes to contribute bandwidth for improved quality-of-service. This work uses market-pricing techniques and virtual currency to ensure effective bandwidth usage and network utilization, while still preventing cheating.

2005–present

Anycast. Designed and built OASIS, a server-selection infrastructure that provides locality- and load-based anycast for replicated Internet services [4] [26]. OASIS tackles the problems of leveraging disparate services to perform (potentially error-prone) network measurement and of scalably managing state information about many services and their participating nodes. OASIS has been in production use since Nov. 2005 and has been adopted by more than a dozen distributed services, handling thousands of replicas. Performed background studies of the geographic locality of IP prefixes [6] and the efficacy of virtual coordinate systems [17]. `http://oasis.coralcdn.org/`

2006–present

IP analytics. By instrumenting CoralCDN, used active web content to measure and analyze the characteristics of over 7 million clients with respect to "edge technologies" (NATs, proxies, DNS and DHCP) [2]. Results quantify how Internet services can use IP addresses to identify clients and enforce access-control decisions. Commercialized historical and real-time techniques for proxy detection and IP geolocation; acquired by Quova, Inc. in Nov. 2006 and currently being tested at large Internet services. `http://illuminati.coralcdn.org/`

2006–present	**Enterprise networks.** Design and implementation contributions to Ethane [3] [1], a backwards-compatible protection and management architecture for enterprise networks. Ethane network switches provide connectivity through on-demand virtual circuits, yet they enforce security policies on a per-flow basis through centrally-managed, atomic, auditable name bindings. Deployment at Stanford since Nov. 2006, serving hundreds of hosts. `http://yuba.stanford.edu/ethane/`
2005–present	**Reliable email.** Designed and implemented the security and privacy protections in Re:, an email acceptance system that leverages social proximity for automated whitelisting [5], using private matching [10]. Recent analysis of privacy for social networks led to more efficient protocols based only on symmetric-key operations (or achieving stronger properties using bilinear maps) [14].
2005–present	**Fault-tolerance groups.** Researched abstractions for the scalable construction of fault-tolerant, distributed systems [15]. Ongoing work with L. Subramanian on partitioning large, dynamic systems into smaller groups, which apply fault-tolerance or reliable communication protocols.
2000–present	**Privacy-preserving protocols.** Developed cryptographic protocols for private matching (PM), which computes the set intersection between two or more parties' inputs [10]. PM uses the properties of homomorphic encryption to privately evaluate a polynomial representation of input sets. Subsequent work led to improved constructions for keyword search (KS) based on oblivious pseudorandom functions [8]. Earlier research included the design and implementation of a prototype system for anonymous cryptographic e-cash (with S. Brands and I. Goldberg), as well as considerations for privacy-enabled digital rights management (DRM) systems [20] [23].
2000–2002	**Anonymity systems.** Designed and implemented Tarzan [13] [21], a peer-to-peer anonymous IP network layer that is strongly resistant to traffic analysis. Helped design Free Haven, a distributed system for the anonymous publishing, storage, and retrieval of information [24] [25] [28].

Positions

3/06–present	**Co-founder** (with Martin Casado). Illuminics Systems, Mountain View, CA.
9/05–present	**Research Assistant.** Stanford University (SCS Group), Stanford, CA.
5/05–8/05	**Research Assistant.** University of California, Berkeley, Berkeley, CA.
9/02–5/05	**Research Assistant.** New York University (SCS Group), New York, NY.
5/03–8/03	**Research Associate.** HP Labs (Trusted Systems Lab), Princeton, NJ.
9/01–6/02	**Research Assistant.** MIT LCS (PDOS Group), Cambridge, MA.
5/01–8/01	**Research Intern.** InterTrust Technologies (STAR Lab), Santa Clara, CA.
6/00–8/00	**Research Intern.** Zero-Knowledge Systems Labs, Montreal, Quebec.
2/99–5/01	**Undergrad Researcher.** MIT LCS (SLS and CIS Groups), Cambridge, MA.
6/99–8/99	**Intern.** Sun Microsystems (HPC Group), Burlington, MA.
6/98–8/98	**Intern.** Cognex Corporation, Natick, MA.
6/96–2/98	**Undergrad Researcher.** MIT Francis Bitter Magnet Lab, Cambridge, MA.

Service

5/03–5/05	**Founder and Organizer.** NYU Systems Reading Group, New York, NY.
2/04–5/05	**Faculty Representative.** NYU Courant Student Organization, New York, NY.
9/01–5/02	**Co-organizer.** MIT Applied Security Reading Group, Cambridge, MA.
9/97–5/02	**President, VP, Winter School Organizer.** MIT Outing Club, Cambridge, MA

Teaching

1/04–5/04	**Teaching Assistant, Lab Instructor.** V22.0480—Computer Networks, NYU.
2/02–5/02	**Teaching Assistant.** 6.033—Computer System Engineering, MIT.
2/01–5/01	**Teaching Assistant.** 6.033—Computer System Engineering, MIT

Advising

Masters	Justin Pettit (Stanford), Robert Soule (NYU), Jeff Borden (NYU)
Undergraduates	Jeffrey Spehar (Stanford), Kevin Shanahan (NYU), Ed Kupershlak (NYU)

Professional activities

Program comm.	WORLDS '06, UPGRADE-CDN '06, IRIS Student P2P Workshop '03
External reviews	NSDI '07, LATIN '06, HotNets '05, EUROCRYPT '05, Usenix Technical '05, ISC '04, CRYPTO '04, IPDPS '04, INFOCOM '04, CCS '03, SOSP '03, ISC '03, PODC '03, EUROCRYPT '03, WPES '02
Journal reviews	ACM Transactions on Computer Systems (TOCS), Journal of Cryptology, Journal of Parallel and Distributed Computing (JPDC), Handbook of Internet Security - P2P Security (Wiley & Sons), Computer Journal

Honors

NDSEG (DoD) Graduate Fellow, 2002-2005
NYU McCracken Fellow, 2002-2006
Henning Biermann Award, NYU Computer Science, 2005 (for outstanding education and service)

Best demo (OASIS), WORLDS 2005.
First paper (highest-ranked), EUROCRYPT 2004 [10].
Award paper, CCS 2002 [13].

Awarded NSF Graduate Fellowship, 2001
Awarded Gordon Wu Fellowship (Princeton), 2001 ; Sterling Prize Fellowship (Yale), 2001
Awarded Graduate Fellowships (U.C.Berkeley, Carnegie-Mellon, UCSD), 2001

Coca-Cola Scholar, 1997-2001 ; Tylenol Scholar, 1997-1999 ; Big 33 Scholar, 1997-1998
Tau Beta Pi, 2000 ; Eta Kappa Nu, 2000 ; Sigma Xi, 2000 ; Order of Omega, 1999
Congressional Award, Silver (1996) and Bronze (1993) medals

Refereed conference publications

[1] Martin Casado, **Michael J. Freedman**, Justin Pettit, Jianying Luo, Nick McKeown, and Scott Shenker. Ethane: Taking control of the enterprise. In *Proc. ACM SIGCOMM Conference*, Kyoto, Japan, August 2007.

[2] Martin Casado and **Michael J. Freedman**. Peering through the shroud: The effect of edge opacity on IP-based client identification. In *Proc. 4th Symposium on Networked Systems Design and Implementation (NSDI 07)*, pages 173–186, Cambridge, MA, April 2007.

[3] Martin Casado, Tal Garfinkle, Aditya Akella, **Michael J. Freedman**, Dan Boneh, Nick McKeown, and Scott Shenker. SANE: A protection architecture for enterprise networks. In *Proc. 15th USENIX Security Symposium*, pages 137–151, Vancouver, BC, August 2006.

[4] **Michael J. Freedman**, Karthik Lakshminarayanan, and David Mazières. OASIS: Anycast for any service. In *Proc. 3rd Symposium on Networked Systems Design and Implementation (NSDI 06)*, pages 129–142, San Jose, CA, May 2006.

[5] Scott Garriss, Michael Kaminsky, **Michael J. Freedman**, Brad Karp, David Mazières, and Haifeng Yu. Re: Reliable email. In *Proc. 3rd Symposium on Networked Systems Design and Implementation (NSDI 06)*, pages 297–310, San Jose, CA, May 2006.

[6] **Michael J. Freedman**, Mythili Vutukuru, Nick Feamster, and Hari Balakrishnan. Geographic locality of IP prefixes. In *Proc. 5th ACM SIGCOMM Conference on Internet Measurement (IMC 05)*, pages 153–158, Berkeley, CA, October 2005.

[7] Siddhartha Annapureddy, **Michael J. Freedman**, and David Mazières. Shark: Scaling file servers via cooperative caching. In *Proc. 2nd Symposium on Networked Systems Design and Implementation (NSDI 05)*, pages 129–142, Boston, MA, May 2005.

[8] **Michael J. Freedman**, Yuval Ishai, Benny Pinkas, and Omer Reingold. Keyword search and oblivious pseudorandom function. In *Proc. 2nd Theory of Cryptography Conference (TCC 05)*, pages 303–324, Cambridge, MA, February 2005.

[9] Yevgeniy Dodis, **Michael J. Freedman**, Stanislaw Jarecki, and Shabsi Walfish. Versatile padding schemes for joint signature and encryption. In *Proc. 11th ACM Conference on Computer and Communication Security (CCS 04)*, pages 344–353, Washington, D.C., October 2004.

[10] **Michael J. Freedman**, Kobbi Nissim, and Benny Pinkas. Efficient private matching and set intersection. In *Advances in Cryptology — EUROCRYPT 2004*, pages 1–19, Interlaken, Switzerland, May 2004.

[11] Maxwell Krohn, **Michael J. Freedman**, and David Mazières. On-the-fly verification of rateless erasure codes for efficient content distribution. In *Proc. IEEE Symposium on Security and Privacy*, pages 226–240, Oakland, CA, May 2004.

[12] **Michael J. Freedman**, Eric Freudenthal, and David Mazières. Democratizing content publication with Coral. In *Proc. 1st Symposium on Networked Systems Design and Implementation (NSDI 04)*, pages 239–252, San Francisco, CA, March 2004.

[13] **Michael J. Freedman** and Robert Morris. Tarzan: A peer-to-peer anonymizing network layer. In *Proc. 9th ACM Conference on Computer and Communications Security (CCS 2002)*, pages 193–206, Washington, D.C., November 2002.

Refereed workshop publications

[14] **Michael J. Freedman** and Antonio Nicolosi. Efficient private techniques for verifying social proximity. In *Proc. 6th International Workshop on Peer-to-Peer Systems (IPTPS 07)*, Bellevue, WA, February 2007.

[15] **Michael J. Freedman**, Ion Stoica, David Mazières, and Scott Shenker. Group therapy for systems: Using link-attestations to manage failures. In *Proc. 5th International Workshop on Peer-to-Peer Systems (IPTPS 06)*, Santa Barbara, CA, February 2006.

[16] **Michael J. Freedman**, Karthik Lakshminarayanan, Sean Rhea, and Ion Stoica. Non-transitive connectivity and DHTs. In *Proc. 2nd Workshop on Real, Large, Distributed Systems (WORLDS 05)*, pages 55–60, San Francisco, CA, December 2005.

[17] Kevin Shanahan and **Michael J. Freedman**. Locality prediction for oblivious clients. In *Proc. 4th International Workshop on Peer-to-Peer Systems (IPTPS 05)*, pages 252–263, Ithaca, NY, February 2005.

[18] Max Krohn and **Michael J. Freedman**. On-the-fly verification of erasure-encoded file transfers (extended abstract). In *Proc. 1st IRIS Student Workshop on Peer-to-Peer Systems*, Cambridge, MA, August 2003.

[19] **Michael J. Freedman** and David Mazières. Sloppy hashing and self-organizing clusters. In *Proc. 2nd International Workshop on Peer-to-Peer Systems (IPTPS 03)*, pages 45–55, Berkeley, CA, February 2003.

[20] Joan Feigenbaum, **Michael J. Freedman**, Tomas Sander, and Adam Shostack. Economic barriers with existing privacy technologies in e-commerce systems. In *Proc. Workshop on Economics and Information Security*, Berkeley, CA, May 2002.

[21] **Michael J. Freedman**, Emil Sit, Josh Cates, and Robert Morris. Introducing Tarzan, a peer-to-peer anonymizing network layer. In *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS 02)*, pages 121–129, Cambridge, MA, March 2002.

[22] **Michael J. Freedman** and Radek Vingralek. Efficient peer-to-peer lookup based on a distributed trie. In *Proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS 02)*, pages 66–75, Cambridge, MA, March 2002.

[23] Joan Feigenbaum, **Michael J. Freedman**, Tomas Sander, and Adam Shostack. Privacy engineering in digital rights management systems. In *Proc. ACM Workshop in Security and Privacy in Digital Rights Management (DRM 01)*, pages 76–105, Philadelphia, PA, November 2001.

[24] Roger Dingledine, **Michael J. Freedman**, David Hopwood, and David Molnar. A reputation system to increase MIX-net reliability. In *Proc. Information Hiding Workshop (LNCS 2137)*, pages 126–141, Pittsburgh, PA, March 2001.

[25] Roger Dingledine, **Michael J. Freedman**, and David Molnar. The Free Haven Project: Distributed anonymous storage service. In *Proc. Workshop on Design Issues in Anonymity and Unobservability (LNCS 2009)*, pages 67–95, Berkeley, CA, July 2000.

Unrefereed publications, book chapters

[26] **Michael J. Freedman**. Automating server selection with OASIS. In *;login: The USENIX Magazine*, pages 46–52, October 2006.

[27] Roger Dingledine, **Michael J. Freedman**, David Molnar, and David Parkes. Reputation. In *Digital Government Civic Scenario Workshop*, Cambridge, MA, April 2003.

[28] Roger Dingledine, **Michael J. Freedman**, and David Molnar. *Peer-to-Peer: Harnessing the Power of Disruptive Technology*, chapter Accountability, pages 271–340. O'Reilly, 2001.

[29] Roger Dingledine, **Michael J. Freedman**, and David Molnar. *Peer-to-Peer: Harnessing the Power of Disruptive Technology*, chapter Free Haven, pages 159–190. O'Reilly, 2001.

References

Prof. David Mazières
Stanford University
Computer Science Department
353 Serra Mall, #290
Stanford, CA 94305-9025
(650) 723-8777
`rec@nospam.scs.stanford.edu`

Prof. Frans Kaashoek
Massachusetts Institute of Technology
Stata Center, #32-G992
77 Massachusetts Avenue
Cambridge, MA 02139
(617) 253-7149
`kaashoek@csail.mit.edu`

Prof. Ion Stoica
University of California, Berkeley
RADLab, Room 465
Soda Hall #1776
Berkeley, CA 94720-1776
(510) 643-4007
`istoica@cs.berkeley.edu`

Prof. Nick McKeown
Stanford University
Computer Science Department
353 Serra Mall, #340
Stanford, CA 94305-9025
(650) 725-3641
`nickm@stanford.edu`

Prof. Joan Feigenbaum
Yale University
Computer Science Department
P.O. Box 208285,
New Haven, CT 06520-8285
(203) 432-6432
`joan.feigenbaum@yale.edu`

Stanford, CA, May 3, 2007