

VITA
Keith B. Frikken

GENERAL INFORMATION

Contact Information

Office: Benton Hall 205C
Mail: Miami University Computer Science and Systems Analysis Department
Oxford, OH 45056
Office phone: (513) 529-0355
Email: frikkekb@muohio.edu

Personal Information

U.S. Citizen
Married
Born 1979

Education

Ph.D. Computer Sciences, Purdue University, 2005 (advisor: Mikhail Atallah), GPA: 4.0.
B.S., Computer Sciences with second major in Mathematics, Winona State University, 2000 (advisor: Gerald Cichanowski), GPA: 4.0.

Other Professional Experience

2006-	Assistant Professor	Miami University
2005-2006	Visiting Assistant Professor	Purdue University
2004-	Member	PriProTex, LLC
2004-2005	Intel Fellow	Purdue University
2002-2004	Research Assistant	Purdue University
2002	Teaching Assistant	Purdue University
2000-2003	GAANN Fellow	Purdue University
2000	Intern	IBM
1998-2000	Industry Experience	WSU Software Testing Lab

Research Interests

- Information Security - protocols, access control, digital rights management, privacy, sensor networks
- Databases - information retrieval, data anonymization

Awards/Honors:

CERIAS Diamond Award Recipient (2005)
Intel Fellowship recipient (2004-2005)
GAANN fellowship recipient (2000-2003)
Fred and Sandy Olson Scholarship (1999)
Presidential Honors Scholarship (1998)
USA Math Olympiad Honorable Mention (1997)

TEACHING

Teaching Experience:

CSA 485/585 Advanced Databases	Spring 2008	Miami U.	Inst Eval: 3.8/4
CSA 271 Object-Oriented Prog	Spring 2008	Miami U.	Inst Eval: 3.6/4
CSA 620I Applied Cryptography	Fall 2008	Miami U.	Inst Eval: 4/4
CSA 271 Object-Oriented Prog	Fall 2008	Miami U.	Inst Eval: 3.4/4
CSA 271 Object-Oriented Prog	Spring 2007	Miami U.	Inst Eval: 3.5/4
CSA 271 Object-Oriented Prog	Spring 2007	Miami U.	Inst Eval: 3.3/4
CSA 271 Object-Oriented Prog	Fall 2006	Miami U.	Inst Eval: 3.3/4
CS 426 Computer Security	Spring 2006	Purdue U.	Inst Eval: 4.5/5
CS 426 Computer Security	Fall 2005	Purdue U.	Inst Eval: 4.7/5
CS 182 Foundations of Comp Sci	Summer 2002	Purdue U.	Inst Eval: 4.6/5

PUBLICATIONS

Book Chapters

1. Mikhail Atallah, Keith Frikken, Carrie Black, Susan Overstreet, and Pooja Bhatia. "Digital Rights Management". The Practical Handbook of Internet Computing, Munindar P. Singh (Ed.), CRC Press, 2004.
2. Mikhail Atallah and Keith Frikken. Privacy-Preserving Cryptographic Protocols. Digital Privacy Theories, Technologies, and Practices, Alessandro Acquisiti, Stefanos Gritzalis, Costas Lambrinouidakis, and Sabrina e Capitani di Vimercati (eds), Auerbach, 2008.

Refereed Publications (accepted or appeared)

Journal Publication

3. M. Atallah, M. Blanton, N. Fazio, and K. Frikken, Dynamic and Efficient Key Management for Access Hierarchies, ACM Transactions on Information and System Security (TISSEC), Conditionally accepted.
4. Danfeng Yao, Keith Frikken, Mike Atallah, Roberto Tamassia. Private Information:

To Reveal or Not To Reveal. ACM Transactions on Information and System Security. Accepted as of July 2008.

5. Keith Frikken, Mikhail Atallah, and Jiangtao Li. "Attribute-Based Access Control with Hidden Policies and Hidden Credentials" IEEE Trans. Computers 55(10): 1259-1270 (2006)
6. Mikhail Atallah, Sunil Prabhakar, Keith Frikken, Radu Sion, "Digital Rights Protection", IEEE Data Engineering Bulletin 27, (2004). Pages 19-26.

Conference Publications

3. Mikhail J. Atallah, Keith B. Frikken, Marina Blanton, YounSun Cho: Private combinatorial group testing. ASIACCS 2008: 312-320. (acceptance rate = 18%).
4. Keith B. Frikken, Joseph A. Dougherty IV. "An efficient integrity-preserving scheme for hierarchical sensor aggregation". WISEC 2008: 68-76. (acceptance for full papers rate = 17%).
5. Keith B. Frikken and Lukasz Opyrchal. "PBS: Private Bartering System". FC 2008. (acceptance rate = 20%).
6. Mikhail J. Atallah, Marina Blanton, and Keith B. Frikken. "Incorporating Temporal Capabilities in Existing Key Management Schemes". ESORICS 2007: 515-530. (acceptance rate = 24%).
7. Keith B. Frikken, "Privacy-Preserving Set Union", In 5th International Conference on Applied Cryptography and Network Security (ACNS'07), June 2007. (acceptance rate = 12%).
8. Mikhail J. Atallah, Marina Blanton, and Keith B. Frikken, "Efficient Techniques for Realizing Geo-Spatial Access Control", In proceedings of ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), Mar. 2007 (acceptance rate = 18%).
9. Danfeng Yao, Keith B. Frikken, Mikhail J. Atallah, and Roberto Tamassia. Point-Based Trust: Define How Much Privacy Is Worth. Accepted for publication in the International Conference on Information and Communications Security (ICICS 2006) (acceptance rate = 18%). Won Best Student Paper Award.
10. Keith Frikken and Philippe Golle. "Private Social Network Analysis: How to Assemble Pieces of a Graph Privately". In proceedings of the 5th annual *ACM Workshop on Privacy in the Electronic Society* (WPES 2006), October 30, 2006. (Acceptance rate = $9/39=23\%$).
11. Keith Frikken, Jiangtao Li, and Mikhail Atallah. "Trust Negotiation with Hidden Credentials, Hidden Policies, and Policy Cycles". Accepted for publication in The 13th Annual Network and Distributed System Security Symposium (NDSS'06). (Acceptance rate = 14%).

12. M. Atallah, M. Blanton, and K. Frikken, “Key Management for Non-Tree Access Hierarchies”. Symposium on Access Control Models and Technologies (SACMAT 2006), pp. 11-18, Jun. 2006. (Acceptance rate = 30%).
13. Mikhail Atallah, Marina Blanton, Keith Frikken, and Jiangtao Li. “Efficient Correlated Action Selection”. In proceedings of Financial Cryptography and Data Security, Feb. 2006. (Acceptance rate = 20%).
14. M. Atallah, M. Blanton, V. Deshpande, K. Frikken, J. Li, and L. Schwarz, “Secure Collaborative Planning, Forecasting, and Replenishment (SCPFR)”. Multi-Echelon/Public Applications of Supply Chain Management Conference, Jun. 2006. Also appeared at Manufacturing and Service Operation Management (M&SOM), Jun. 2005.
15. Mikhail Atallah, Keith Frikken, and Marina Blanton. “Dynamic and Efficient Key Management for Access Hierarchies”. In the 12th annual ACM Conference on Computer and Communications Security (CCS’05). (Acceptance rate 38/249=15%).
16. Keith Frikken. “Optimal Distributed Declustering using Replication”. In *Tenth International Conference on Database Theory (ICDT 2005)*. Pages 144-157. January 5-7, 2005. (Acceptance rate 24/84=29%)
17. Keith Frikken and Mikhail Atallah. “Achieving Fairness in Private Contract Negotiation”. In the Ninth Internal Conference on *Financial Cryptography and Data Security (FC 2005)*, Feb 28-Mar 3, 2005. (Acceptance rate 24/90=26%)
18. Mikhail Atallah, Keith Frikken, Michael T. Goodrich, and Roberto Tamassia. “Secure Biometric Authentication for Weak Computational Devices”. In the Ninth Internal Conference on *Financial Cryptography and Data Security (FC 2005)*, Feb 28-Mar 3, 2005. (Acceptance rate 24/90=26%)
19. Keith Frikken, Mikhail Atallah, and Chen Zhang. “Privacy-Preserving Credit Checking”. In the ACM Conference on Electronic Commerce (EC 2005). June 5-8, 2005. (Acceptance rate 33/113=29%).
20. Keith Frikken, Mikhail Atallah, and Marina Bykova. “Remote Revocation of Smart Cards in a Private DRM system”. In *Australasian Information Security Workshop (AISW 2005)*, pages 169-177. Jan31-Feb 3, 2005. (Acceptance rate 13/35=37%)
21. Keith Frikken and Mikhail Atallah. “Privacy Preserving Route Planning”. In the 3rd annual *Workshop on Privacy in the Electronic Society (WPES 2004)*, October 27 - 31, 2004, Washington, D.C. Pages 8-15. (Acceptance rate for full papers, 10/45 = 22%)
22. Marina Bykova, Mikhail Atallah, Jiangtao Li, Keith Frikken, and Mercan Topkara, “Private Collaborative Forecasting and Benchmarking”. In the 3rd annual *Workshop on Privacy in the Electronic Society (WPES 2004)*, October 27 - 31, 2004, Washington, D.C. Pages 103-114. (Acceptance rate for full papers, 10/45 = 22%)
23. Keith Frikken, Mikhail Atallah, and Jiangtao Li. “Hidden Access Control Policies with Hidden Credentials”. Short Paper in the 3rd annual *Workshop on Privacy in the Electronic Society (WPES 2004)*, October 27 - 31, 2004, Washington, D.C. Pages

- 27-28. (Acceptance rate for all papers, $21/45 = 47\%$),
24. Mikhail Atallah and Keith Frikken. "Privacy-Preserving Location Dependent Query Processing". In *Proceeding of ACS/IEEE International Conference on Pervasive Services (ICPS 2004)*. Pages 9-17.
 25. Keith Frikken and Mikhail Atallah. "Privacy Preserving Electronic Surveillance". In the *Workshop on Privacy in the Electronic Society (WPES 2003)*, October 27 - 31, 2003, Washington, D.C. Pages=45-54. (Acceptance rate $16/50 = 32\%$)
 26. Mikhail Atallah and Keith Frikken. "Replicated Parallel I/O without Additional Scheduling Costs". In *Proceedings of 14th International Conference of Database and Expert Systems Applications (DEXA 2003)*. LNCS 2736. Pages = 223-232. (Acceptance rate $91/236 = 39\%$)
 27. Keith Frikken and Mikhail Atallah. "Cropping-Resilient Segmented Multiple Watermarking (Extended Abstract)". In *Proceedings of 8th International Workshop on Algorithms and Data Structures (WADS 2003)*. LNCS 2748. Pages = 231-242. (Acceptance rate $40/126 = 32\%$)
 28. Keith Frikken, Mikhail Atallah, Sunil Prabhakar, and Rei Safavi-Naini. "Optimal Parallel I/O for Range Queries through Replication". In *Proceedings of 13th International Conference of Database and Expert Systems Applications (DEXA 2002)*. LNCS 2453. Pages = 669-678. (Acceptance rate $89/241 = 37\%$)

Presentations

1. "PBS: Private Bartering System". FC 2008
2. "An efficient integrity-preserving scheme for hierarchical sensor aggregation". Wisec 2008
3. "Privacy-Preserving Set Union". ACNS 2007
4. "Private Social Network Analysis: How to Assemble Pieces of a Graph Privately". WPES 2006
5. "Key Management for Non-Tree Access Hierarchies". SACMAT 2006.
6. "Confidentiality in Online Collaborations". Job talk at Towson University's Department of Computer and Information Sciences. February 2006.
7. "Confidentiality in Online Collaborations". Job talk at University of Central Arkansas's Department of Computer Science. February 2006.
8. "Confidentiality in Online Collaborations". Job talk at New Jersey Insitutitute of Technology's Department of Computer Science. January 2006.
9. "Confidentiality in Online Collaborations". Job talk at Northern Kentucky University's Department of Computer Science. January 2006.
10. "Confidentiality in Online Collaborations". Job talk at University of North Texas's

- Department of Computer Science and Engineering. January 2006.
11. “Hidden Access Control Policies with Hidden Credentials”. Job talk at Florida State University’s Department of Computer Science. May 2005.
 12. “Hidden Access Control Policies with Hidden Credentials”. Job talk at Washington University in St. Louis’s Department of Computer Science and Engineering. March 2005.
 13. “Privacy-Preserving Credit Checking”. EC 2005.
 14. “Achieving Fairness in Private Contract Negotiation”. FC 2005.
 15. “Secure Biometric Authentication for Weak Computational Devices”. FC 2005
 16. “Hidden Access Control Policies with Hidden Credentials”. Job talk at Dartmouth College’s Department of Computer Science. February 2005.
 17. “Hidden Access Control Policies with Hidden Credentials”. Job talk at Utah State University’s Department of Computer Science. February 2005.
 18. “Remote Revocation of Smart Cards in a Private DRM system”. AISW 2005.
 19. “Hidden Access Control Policies with Hidden Credentials”. Job talk at University of Notre Dame’s Department of Computer Science and Engineering. January 2005.
 20. “Hidden Access Control Policies with Hidden Credentials”. Job talk at University of Iowa’s Department of Computer Science. January 2005.
 21. “Hidden Access Control Policies with Hidden Credentials”. CERIAS Security Seminar, Purdue University. January 2005.
 22. “Optimal Distributed Declustering using Replication”. ICDT 2005
 23. “Privacy-Preserving Route Planning”. WPES 2004
 24. “Privacy Preserving Electronic Surveillance”. WPES 2003
 25. “Replicated Parallel I/O without Additional Scheduling Costs”. DEXA 2003
 26. “Cropping-Resilient Segmented Multiple Watermarking (Extended Abstract)”. WADS 2003
 27. “Optimal Parallel I/O for Range Queries through Replication”. DEXA 2002

PROFESSIONAL RECONGNITION

Program Committees

1. ACM WPES 2007, 2008 (Workshop for Privacy in the Electronic Society)
2. INSPEC 2008 (International Workshop on Security and Privacy in Enterprise Computing)
3. CISC 2005 (SKLOIS Conference on Information Security and Cryptology)

Refereeing for Journal and Conferences

1. ACNS (Conference on Applied Cryptography and Network Security)
2. ACM EC (Conference on Electronic Commerce)
3. ACM CCS (Conference on Computer and Communications Security)
4. MFCS (Mathematical Foundations of Computer Science)
5. IEEE TPDS (Transactions on Parallel and Distributed Systems)
6. ISAAC (International Symposium on Algorithms and Computation)
7. ACM WPES (Workshop for Privacy in the Electronic Society)
8. ICICS (International Conference on Information and Communications Security)
9. ACM SACMAT (Symposium on Access Control Models and Technologies)
10. WPET (Workshop on Privacy Enhancing Technologies)
11. ACM SIGACT-SIGMOD-SIGART PODS (Symposium on Principles of Database Systems)
12. IEEE TKDE (Transactions on Knowledge and Data Engineering)
13. NDSS (Network and Distributed System Security Symposium)
14. SDCS (International Workshop on Security in Distributed Computing Systems)
15. IEEE TC (Transactions on Computing)
16. PKDD (Principles and Practice of Knowledge Discovery in Databases)
17. ACM SACMAT (Symposium on Access Control Models and Technologies)
18. IPL (Information Processing Letters)
19. ACM DKDM (ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery)
20. IEEE CEC (Conference on Electronic Commerce)

OTHER PROFESSIONAL ACTIVITIES

Administrative Duties

2007–	SEAS Research Council	Miami U.
2007–	CSA Graduate Committe	Miami U.
2006–2007	CSA Library Liaison	Miami U.
2004–2005	School of Science Grade Appeals Committee	Purdue U.

Associations

ACM