Stanford

John Mitchell

Mary and Gordon Crary Family Professor in the School of Engineering, and Professor, by courtesy, of Electrical Engineering and of Education

Computer Science

CONTACT INFORMATION

- **Administrative Contact**

  Uera Smith III

  Email usmith@stanford.edu

Bio

BIO

John Mitchell is the Mary and Gordon Crary Family Professor, professor of computer science, and by courtesy professor of electrical engineering and professor of education. He was previously Stanford Vice Provost for Teaching and Learning and chair of the Computer Science Department. As vice provost, his team worked with more than 500 Stanford faculty members and instructors on over 1,000 online projects for campus or public audiences and organized the Year of Learning to envision the future of teaching and learning at Stanford and beyond. As co-director of the Lytics Lab, Carta Lab and Pathways Lab, he has worked to improve educational outcomes through data-driven research and iterative design.

Mitchell's research focusses on programming languages, computer security and privacy, blockchain, machine learning, and technology for education. Sample publications include Reinforcement Learning for the Adaptive Scheduling of Educational Activities (CHI 2020), Automated Analysis of Cryptographic Assumptions in Generic Group Models (J. Cryptology, 2019), Evaluating the privacy properties of telephone metadata (PNAS 2016), and Third-party web tracking: Policy and Technology (IEEE S&P). He is the author of two textbooks, Foundations for Programming Languages (1996) and Concepts in Programming Languages (2002). With over 250 publications and over 30,000 citations, he has led research projects on a range of topics, been a consultant or advisor to many companies, and served as editor-in-chief of the Journal of Computer Security.

Mitchell's first research project in online learning started in 2009, when he and six undergraduate students built Stanford CourseWare, an innovative platform that expanded to support interactive video and discussion. CourseWare served as the foundation for initial flipped classroom experiments at Stanford and helped inspire the first massive open online courses (MOOCs) from Stanford.

ACADEMIC APPOINTMENTS

- Professor, Computer Science
- Professor (By courtesy), Electrical Engineering
- Professor (By courtesy), Graduate School of Education
- Faculty Affiliate, Institute for Human-Centered Artificial Intelligence (HAI)

ADMINISTRATIVE APPOINTMENTS

- Chair, Department of Computer Science, (2019- present)

HONORS AND AWARDS

- Mary and Gordon Crary Family Professor in the School of Engineering, Stanford University
- Elected, American Academy of Arts and Sciences
- Fellow, Association for Computing Machinery

PROFESSIONAL EDUCATION

- BS, Stanford Univeristy , Mathematics (1978)
- PhD, MIT , Computer Science (1984)

Research & Scholarship

RESEARCH INTERESTS

- Higher Education
- Teachers and Teaching
- Technology and Education

CURRENT RESEARCH AND SCHOLARLY INTERESTS

Programming languages, computer security and privacy, blockchain, machine learning, and technology for education

Teaching

COURSES

2023-24

- Design for Learning: Generative AI for Collaborative Learning: CS 498D, DESIGN 292, EDUC 449 (Aut)
- How Can Generative AI Help Us Learn?: CS 53N (Spr)
- Trustworthy Machine Learning: CS 329T (Aut)

2022-23

- Design for Learning: Co-Designing Connection and Community: DESIGN 292 (Aut)

2021-22

- Trustworthy Machine Learning: CS 329T (Spr)

2020-21

- Minds and Machines: CS 24, LINGUIST 35, PHIL 99, PSYCH 35, SYMSYS 1, SYMSYS 200 (Win)
- Trustworthy Machine Learning: CS 329T (Spr)

STANFORD ADVISEES

Doctoral Dissertation Reader (AC)

Yunsung Kim

Master's Program Advisor

Luke Babbitt, Alex Derhacobian, Hassan Fahmy, Roman Gasiorowski, Jeremy Kim, Calvin Laughlin, Sean Mori, Ihyun Nam, Ayush Singla, Ari Webb

Doctoral (Program)

Sierra Wang

Publications

PUBLICATIONS

- **Remote Learning and Work** *IEEE INTERNET COMPUTING*
  Kizilcec, R., Mitchell, J.
  2024; 28 (1): 7-9
- **Detecting the Reasons for Program Decomposition in CS1 and Evaluating Their Impact** *ACM Technical Symposium on Computer Science Education*
  Charitsis, C., Piech, C., Mitchell, J. C.
  2023: 2023
- **Insights for post-pandemic pedagogy across one CS department**
  Bigman, M., Gilon, Y., Han, J., Mitchell, J. C.
  Arxiv.
  2022
- **Using NLP to quantify program decomposition in CS1** *ACM Conference on Learning @ Scale*
  Charitsis, C., Piech, C., Mitchell, J. C.
  2022: 113-120
- **Function Names: Quantifying the Relationship Between Identifiers and Their Functionality to Improve Them** *ACM Conference on Learning @ Scale*
  Charitsis, C., Piech, C., Mitchell, J. C.
  2022: 93-101
- **Feedback on Program Development Process for CS1 Students** *ACM Technical Symposium on Computer Science Education*
  Charitsis, C., Piech, C., Mitchell, J. C.
  2022: 1150
- **Assessing Function Names and Quantifying the Relationship Between Identifiers and Their Functionality to Improve Them**
  Charitsis, C., Piech, C., Mitchell, J. C.
  2021: 291-293
- **Simplifying Automated Assessment in CS1** *International Conference on Education Technology Management*
  Chartists, C., Piech, C., Mitchell, J. C.
  2021: 226-231
- **Model Checking Bitcoin and other Proof-of-Work Consensus Protocols**
  DiGiacomo-Castillo, M., Liang, ., Pal, A., Mitchell, J. C.
  2020 IEEE International Conference on Blockchain.
  2020
- **Model Checking Bitcoin and other Proof-of-Work Consensus Protocols**
  DiGiacomo-Castillo, M., Liang, Y., Pal, A., Mitchell, J. C., IEEE Comp Soc
  IEEE COMPUTER SOC.2020: 351-358
- **Reinforcement Learning for the Adaptive Scheduling of Educational Activities**
  Bassen, J., Balaji, B., Schaarschmidt, M., Thille, C., Painter, J., Zimmaro, D., Gamest, A., Fast, E., Mitchell, J. C., ACM
  ASSOC COMPUTING MACHINERY.2020
- **Teaching Online in 2020: Experiments, Empathy, Discovery**
  Bigman, M., Mitchell, J. C.
  IEEE Learning With MOOCS (LWMOOCS).
  2020
- **Reinforcement Learning for the Adaptive Scheduling of Educational Activities**
  Bassen, J., Balaji, B., Schaarschmidt, M., Thille, C., Painter, J., Zimmaro, D., Games, A., Fast, E., Mitchell, J. C.
  Proc 2020 CHI Conference on Human Factors in Computing Systems.
  2020

- **Automated Analysis of Cryptographic Assumptions in Generic Group Models** *JOURNAL OF CRYPTOLOGY*
  Barthe, G., Fagerholm, E., Fiore, D., Mitchell, J., Scedrov, A., Schmidt, B.
  2019; 32 (2): 324–60
- **Data Oblivious Genome Variants Search on Intel SGX**
  Mandal, A., Mitchell, J. C., Montgomery, H., Roy, A., GarciaAlfaro, J., HerreraJoancomarti, J., Livraga, G., Rios, R.
  SPRINGER INTERNATIONAL PUBLISHING AG.2018: 296–310
- **Flexible dynamic information flow control in the presence of exceptions** *JOURNAL OF FUNCTIONAL PROGRAMMING*
  Stefan, D., Mazieres, D., Mitchell, J. C., Russo, A.
  2017; 27
- **Privacy for Targeted Advertising**
  Mandal, A., Mitchell, J., Montgomery, H., Roy, A., IEEE
  IEEE.2017: 438–43
- **Hails: Protecting data privacy in untrusted web applications** *JOURNAL OF COMPUTER SECURITY*
  Giffin, D., Levy, A., Stefan, D., Terei, D., Mazieres, D., Mitchell, J., Russo, A.
  2017; 25 (4-5): 427–61
- **Evaluating the privacy properties of telephone metadata** *PROCEEDINGS OF THE NATIONAL ACADEMY OF SCIENCES OF THE UNITED STATES OF AMERICA*
  Mayer, J., Mutchler, P., Mitchell, J. C.
  2016; 113 (20): 5536-5541
- **Target Fragmentation in Android Apps**
  Mutchler, P., Safaei, Y., Doupe, A., Mitchell, J., IEEE
  IEEE.2016: 204–13
- **Fast Algorithms for Learning with Long N-grams via Suffix Tree Based Matrix Multiplication**
  Paskov, H. S., Mitchell, J. C., Hastie, T. J., Meila, M., Heskes, T.
  AUAI PRESS.2015: 672–81
- **Automated Analysis of Cryptographic Assumptions in Generic Group Models**
  Barthe, G., Fagerholm, E., Fiore, D., Mitchell, J., Scedrov, A., Schmidt, B., Garay, J. A., Gennaro, R.
  SPRINGER-VERLAG BERLIN.2014: 95–112
- **Principles of Security and Trust - Second International Conference, POST 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software**
  edited by Basin, David, A., Mitchell, John, C.
  2013
- **Oblivious program execution and path-sensitive non-interference** *IEEE 26th Computer Security Foundations Symposium*
  Planul, J., Mitchell, J. C.
  IEEE.2013: 66–80
- **Oblivious Program Execution and Path-Sensitive Non-interference.**
  Planul, J., Mitchell, John, C.
  2013
- **Compressive Feature Learning.**
  Paskov, Hristo, S., West, R., Mitchell, John, C., Hastie, Trevor, J.
  2013
- **Addressing Covert Termination and Timing Channels in Concurrent Information Flow Systems** *ACM SIGPLAN NOTICES*
  Stefan, D., Russo, A., Buiras, P., Levy, A., Mitchell, J. C., Mazieres, D.
  2012; 47 (9): 201-213
- **A Learning-Based Approach to Reactive Security** *IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING*
  Barth, A., Rubinstein, B. I., Sundararajan, M., Mitchell, J. C., Song, D., Bartlett, P. L.

2012; 9 (4): 482-493

- **Privacy and Cybersecurity: The Next 100 Years** *PROCEEDINGS OF THE IEEE*
  Landwehr, C., Boneh, D., Mitchell, J. C., Bellovin, S. M., Landau, S., Lesk, M. E.
  2012; 100: 1659-1673
- **Third-Party Web Tracking: Policy and Technology.**
  Mayer, Jonathan, R., Mitchell, John, C.
  2012
- **Disjunction Category Labels** *16th Nordic Conference on Secure IT-Systems (NordSec)*
  Stefan, D., Russo, A., Mazieres, D., Mitchell, J. C.
  SPRINGER-VERLAG BERLIN.2012: 223–239
- **Third-Party Web Tracking: Policy and Technology** *33rd IEEE Symposium on Security and Privacy (SP)*
  Mayer, J. R., Mitchell, J. C.
  IEEE.2012: 413–427
- **Information-flow control for programming on encrypted data** *25th IEEE Computer Security Foundations Symposium (CSF)*
  Mitchell, J. C., Sharma, R., Stefan, D., Zimmerman, J.
  IEEE.2012: 45–60
- **SessionJuggler: secure web login from an untrusted terminal using session hijacking.**
  Bursztein, E., Soman, C., Boneh, D., Mitchell, John, C.
  2012
- **Addressing covert termination and timing channels in concurrent information flow systems.**
  Stefan, D., Russo, A., Buiras, P., Levy, A., Mitchell, John, C., Mazières, D.
  2012
- **Declarative privacy policy: finite models and attribute-based encryption.**
  Lam, Peifung, E., Mitchell, John, C., Scedrov, A., Sundaram, S., Wang, F.
  2012
- **Information-Flow Control for Programming on Encrypted Data.**
  Mitchell, John, C., Sharma, R., Stefan, D., Zimmerman, J.
  2012
- **Information-flow control for programming on encrypted data.** *IACR Cryptology ePrint Archive*
  Mitchell, John, C., Sharma, R., Stefan, D., Zimmerman, J.
  2012: 205
- **Flexible Dynamic Information Flow Control in the Presence of Exceptions.** *CoRR abs/1207.1457*
  Stefan, D., Russo, A., Mitchell, John, C., Mazières, D.
  2012
- **Flexible Dynamic Information Flow Control in Haskell** *ACM SIGPLAN NOTICES*
  Stefan, D., Russo, A., Mitchell, J. C., Mazieres, D.
  2011; 46 (12): 95-106
- **A 1-year follow-up of a multi-center treatment trial of adults with anorexia nervosa** *EATING AND WEIGHT DISORDERS-STUDIES ON ANOREXIA BULIMIA AND OBESITY*
  Yu, J., Agras, W. S., HALMI, K. A., Crow, S., Mitchell, J., Bryson, S. W.
  2011; 16 (3): E177-E181
- **Security Modeling and Analysis** *IEEE SECURITY & PRIVACY*
  Bau, J., Mitchell, J. C.
  2011; 9 (3): 18-25
- **A Symbolic Logic with Exact Bounds for Cryptographic Protocols.**
  Mitchell, John, C.

2011

- **Flexible Dynamic Information Flow Control in Haskell**
  Stefan, D., Russo, A., Mitchell, J. C., Mazieres, D., ACM
  ASSOC COMPUTING MACHINERY.2011: 95–106
- **Program Analysis for Web Security**
  Mitchell, J. C., Yahav, E.
  SPRINGER-VERLAG BERLIN.2011: 4
- **Text-based CAPTCHA Strengths and Weaknesses**
  Bursztein, E., Martin, M., Mitchell, J. C., ACM
  ASSOC COMPUTING MACHINERY.2011: 125–37
- **A Domain-Specific Language for Computing on Encrypted Data**
  Bain, A., Mitchell, J., Sharma, R., Stefan, D., Zimmerman, J., Chakraborty, S., Kumar, A.
  SCHLOSS DAGSTUHL, LEIBNIZ CENTER INFORMATICS.2011: 6–24
- **The Failure of Noise-Based Non-Continuous Audio Captchas** *32nd IEEE Symposium on Security and Privacy (SP 2011)*
  Bursztein, E., Beauxis, R., Paskov, H., Perito, D., Fabry, C., Mitchell, J.
  IEEE COMPUTER SOC.2011: 19–31
- **Reclaiming the Blogosphere, TalkBack: A Secure LinkBack Protocol for Weblogs** *16th European Symposium on Research in Computer Security (ESORICS 2011)*
  Bursztein, E., Gourdin, B., Mitchell, J. C.
  SPRINGER-VERLAG BERLIN.2011: 133–149
- **A Symbolic Logic with Exact Bounds for Cryptographic Protocols** *18th Workshop on Logic, Language, Information and Computation (WoLLIC)*
  Mitchell, J. C.
  SPRINGER-VERLAG BERLIN.2011: 3–3
- **Automated Analysis of Security-Critical JavaScript APIs** *32nd IEEE Symposium on Security and Privacy (SP 2011)*
  Taly, A., Erlingsson, U., Mitchell, J. C., Miller, M. S., Nagra, J.
  IEEE COMPUTER SOC.2011: 363–378
- **Automated Analysis of Security-Critical JavaScript APIs.**
  Taly, A., Erlingsson, Ú., Mitchell, John, C., Miller, Mark, S., Nagra, J.
  2011
- **The Failure of Noise-Based Non-continuous Audio Captchas.**
  Bursztein, E., Beauxis, R., Paskov, Hristo, S., Perito, D., Fabry, C., Mitchell, John, C.
  2011
- **Program Analysis for Web Security.**
  Mitchell, John, C.
  2011
- **Disjunction Category Labels.**
  Stefan, D., Russo, A., Mazières, D., Mitchell, John, C.
  2011
- **Reclaiming the Blogosphere, TalkBack: A Secure LinkBack Protocol for Weblogs.**
  Bursztein, E., Gourdin, B., Mitchell, John, C.
  2011
- **Text-based CAPTCHA strengths and weaknesses.**
  Bursztein, E., Martin, M., Mitchell, John, C.
  2011
- **TBA : A Hybrid of Logic and Extensional Access Control Systems.** *Formal Aspects in Security and Trust*
  Hinrichs, Timothy, L., Garrison III, William, C., Lee, Adam, J., Saunders, S., Mitchell, John, C.

2011

- **A Domain-Specific Language for Computing on Encrypted Data.** *IACR Cryptology ePrint Archive*
  Bain, A., Mitchell, John, C., Sharma, R., Stefan, D., Zimmerman, J.
  2011: 561
- **Inductive trace properties for computational security.** *Journal of Computer Security*
  Roy, A., Datta, A., Derek, A., Mitchell, John, C.
  2010; 6 (18): 1035-1073
- **Inductive trace properties for computational security** *JOURNAL OF COMPUTER SECURITY*
  Roy, A., Datta, A., Derek, A., Mitchell, J.
  2010; 18 (6): 1035–73
- **A Learning-Based Approach to Reactive Security** *14th Financial Cryptography and Data Security International Conference*
  Barth, A., Rubinstein, B. I., Sundararajan, M., Mitchell, J. C., Song, D., Bartlett, P. L.
  SPRINGER-VERLAG BERLIN.2010: 192–206
- **Using Strategy Objectives for Network Security Analysis** *5th China International Conference on Information Security and Cryptology*
  Bursztein, E., Mitchell, J. C.
  SPRINGER-VERLAG BERLIN.2010: 337–349
- **State of the Art: Automated Black-Box Web Application Vulnerability Testing** *Symposium on Security and Privacy*
  Bau, J., Bursztein, E., Gupta, D., Mitchell, J.
  IEEE COMPUTER SOC.2010: 332–345
- **Towards a Formal Foundation of Web Security** *23rd IEEE Computer Security Foundations Symposium (CSF)/Federated Logic Conference*
  Akhawe, D., Barth, A., Lam, P. E., Mitchell, J., Song, D.
  IEEE COMPUTER SOC.2010: 290–304
- **Object Capabilities and Isolation of Untrusted Web Applications** *Symposium on Security and Privacy*
  Maffeis, S., Mitchell, J. C., Taly, A.
  IEEE COMPUTER SOC.2010: 125–140
- **How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation** *Symposium on Security and Privacy*
  Bursztein, E., Bethard, S., Fabry, C., Mitchell, J. C., Jurafsky, D.
  IEEE COMPUTER SOC.2010: 399–413
- **A Security Evaluation of DNSSEC with NSEC3.** *IACR Cryptology ePrint Archive*
  Bau, J., Mitchell, John, C.
  2010: 115
- **A Learning-Based Approach to Reactive Security.** *Financial Cryptography*
  Barth, A., Rubinstein, Benjamin, I. P., Sundararajan, M., Mitchell, John, C.
  2010
- **A Security Evaluation of DNSSEC with NSEC3.**
  Bau, J., Mitchell, John, C.
  2010
- **How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation.**
  Bursztein, E., Bethard, S., Fabry, C., Mitchell, John, C., Jurafsky, D.
  2010
- **State of the Art: Automated Black-Box Web Application Vulnerability Testing.**
  Bau, J., Bursztein, E., Gupta, D., Mitchell, John, C.
  2010
- **Object Capabilities and Isolation of Untrusted Web Applications.**
  Maffeis, S., Mitchell, John, C., Taly, A.

2010

- **Towards a Formal Foundation of Web Security.**
  Akhawe, D., Barth, A., Lam, Peifung, E., Mitchell, John, C., Song, D.
  2010
- **A 4-Year Prospective Study of Eating Disorder NOS Compared with Full Eating Disorder Syndromes** *INTERNATIONAL JOURNAL OF EATING DISORDERS*
  Agras, W. S., Crow, S., Mitchell, J. E., Halmi, K. A., Bryson, S.
  2009; 42 (6): 565-570
- **Securing Frame Communication in Browsers** *COMMUNICATIONS OF THE ACM*
  Barth, A., Jackson, C., Mitchell, J. C.
  2009; 52 (6): 83-91
- **An Automated Approach for Proving PCL Invariants** *ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE*
  Mitchell, J. C., Roy, A., Sundararajan, M.
  2009; 234: 93–113
- **Isolating JavaScript with Filters, Rewriting, and Wrappers.**
  Maffeis, S., Mitchell, John, C., Taly, A.
  2009
- **Isolating JavaScript with Filters, Rewriting, and Wrappers** *COMPUTER SECURITY - ESORICS 2009, PROCEEDINGS*
  Maffeis, S., Mitchell, J. C., Taly, A.
  2009; 5789: 505-?
- **A Formalization of HIPAA for a Medical Messaging System.**
  Lam, Peifung, E., Mitchell, John, C., Sundaram, S.
  2009
- **A Learning-Based Approach to Reactive Security.** *CoRR abs/0912.1155*
  Barth, A., Rubinstein, Benjamin, I. P., Sundararajan, M., Mitchell, John, C., Song, D. X., Bartlett, Peter, L.
  2009
- **Practical declarative network management.**
  Hinrichs, Timothy, L., Gude, N., Casado, M., Mitchell, John, C., Shenker, S.
  2009
- **TrackBack spam: abuse and prevention.**
  Bursztein, E., Lam, Peifung, E., Mitchell, John, C.
  2009
- **An Automated Approach for Proving PCL Invariants.** *Electr. Notes Theor. Comput. Sci.*
  Mitchell, John, C., Roy, A., Sundararajan, M.
  2009; 234: 93-113
- **Using Strategy Objectives for Network Security Analysis.**
  Bursztein, E., Mitchell, John, C.
  2009
- **On the relationships between notions of simulation-based security** *JOURNAL OF CRYPTOLOGY*
  Kuesters, R., Datta, A., Mitchell, J. C., Ramanathan, A.
  2008; 21 (4): 492-546
- **A Layered Architecture for Detecting Malicious Behaviors.**
  Martignoni, L., Stinson, E., Fredrikson, M., Jha, S., Mitchell, John, C.
  2008
- **A Layered Architecture for Detecting Malicious Behaviors** *RECENT ADVANCES IN INTRUSION DETECTION, RAID 2008*
  Martignoni, L., Stinson, E., Fredrikson, M., Jha, S., Mitchell, J. C.

2008; 5230: 78-?

- **An Operational Semantics for JavaScript** *PROGRAMMING LANGUAGES AND SYSTEMS, PROCEEDINGS*
  Maffeis, S., Mitchell, J. C., Taly, A.
  2008; 5356: 307-?
- **Analysis of EAP-GPSK Authentication Protocol.**
  Mitchell, John, C., Roy, A., Rowe, P., Scedrov, A.
  2008
- **Securing Frame Communication in Browsers.**
  Barth, A., Jackson, C., Mitchell, John, C.
  2008
- **An Operational Semantics for JavaScript.**
  Maffeis, S., Mitchell, John, C., Taly, A.
  2008
- **Robust defenses for cross-site request forgery.**
  Barth, A., Jackson, C., Mitchell, John, C.
  2008
- **Characterizing Bots' Remote Control Behavior.** *Botnet Detection*
  Stinson, E., Mitchell, John, C.
  2008: 45-64
- **Towards Systematic Evaluation of the Evadability of Bot/Botnet Detection Methods.**
  Stinson, E., Mitchell, John, C.
  2008
- **Protocol Composition Logic (PCL)** *ELECTRONIC NOTES IN THEORETICAL COMPUTER SCIENCE*
  Datta, A., Derek, A., Mitchell, J. C., Roy, A.
  2007; 172: 311–58
- **Characterizing Bots' Remote Control Behavior.**
  Stinson, E., Mitchell, John, C.
  2007
- **Protocol Composition Logic (PCL).** *Electr. Notes Theor. Comput. Sci.*
  Datta, A., Derek, A., Mitchell, John, C., Roy, A.
  2007; 172: 311-358
- **Inductive Proof Method for Computational Secrecy.** *IACR Cryptology ePrint Archive*
  Roy, A., Datta, A., Derek, A., Mitchell, John, C.
  2007: 165
- **Privacy and Utility in Business Processes.**
  Barth, A., Mitchell, John, C., Datta, A., Sundaram, S.
  2007
- **Formal Proofs of Cryptographic Security of Diffie-Hellman-Based Protocols.**
  Roy, A., Datta, A., Mitchell, John, C.
  2007
- **Inductive Proofs of Computational Secrecy.**
  Roy, A., Datta, A., Derek, A., Mitchell, John, C.
  2007
- **Compositional analysis of contract-signing protocols** *2nd Workshop on Automated Reasoning for Security Protocol Analysis*
  Backes, M., Datta, A., Derek, A., Mitchell, J. C., Turuani, M.

ELSEVIER SCIENCE BV.2006: 33–56

- **A probabilistic polynomial-time process calculus for the analysis of cryptographic protocols** *THEORETICAL COMPUTER SCIENCE*
  Mitchell, J. C., Ramanathan, A., Scedrov, A., Teague, V.
  2006; 353 (1-3): 118-164
- **Games and the Impossibility of Realizable Ideal Functionality.**
  Datta, A., Derek, A., Mitchell, John, C., Ramanathan, A., Scedrov, A.
  2006
- **Secrecy Analysis in Protocol Composition Logic.**
  Roy, A., Datta, A., Derek, A., Mitchell, John, C., Seifert, J.
  2006
- **Protecting browser state from web privacy attacks.**
  Jackson, C., Bortz, r., Boneh, D., Mitchell, John, C.
  2006
- **Computationally Sound Compositional Logic for Key Exchange Protocols.**
  Datta, A., Derek, A., Mitchell, John, C., Warinschi, B.
  2006
- **Inductive Trace Properties for Computational Security.** *IACR Cryptology ePrint Archive*
  Roy, A., Datta, A., Derek, A., Mitchell, John, C.
  2006: 486
- **On the Relationships Between Notions of Simulation-Based Security.** *IACR Cryptology ePrint Archive*
  Datta, A., Küsters, R., Mitchell, John, C., Ramanathan, A.
  2006: 153
- **Understanding SPKI/SDSI using first-order logic.** *Int. J. Inf. Sec.*
  Li, N., Mitchell, John, C.
  2006; 1 (5): 48-64
- **Managing Digital Rights using Linear Logic.**
  Barth, A., Mitchell, John, C.
  2006
- **Privacy and Contextual Integrity: Framework and Applications.**
  Barth, A., Datta, A., Mitchell, John, C., Nissenbaum, H.
  2006
- **Key Exchange Protocols: Security Definition, Proof Method and Applications.** *IACR Cryptology ePrint Archive*
  Datta, A., Derek, A., Mitchell, John, C., Warinschi, B.
  2006: 56
- **Contract signing, optimism, and advantage** *JOURNAL OF LOGIC AND ALGEBRAIC PROGRAMMING*
  CHADHA, R., Mitchell, J. C., Scedrov, A., Shmatikov, V.
  2005; 64 (2): 189-218
- **Beyond proof-of-compliance: Security analysis in trust management** *JOURNAL OF THE ACM*
  Li, N. H., Mitchell, J. C., Winsborough, W. H.
  2005; 52 (3): 474-514
- **Probabilistic polynomial-time semantics for a protocol security logic** *32nd International Colloquium on Automata, Languages and Programming (ICALP 2005)*
  Datta, A., Derek, A., Mitchell, J. C., Shmatikov, V., Turuani, M.
  SPRINGER-VERLAG BERLIN.2005: 16–29
- **LEA derivation system and compositional logic for security protocols** *JOURNAL OF COMPUTER SECURITY*
  Datta, A., Derek, A., Mitchell, J., Pavlovic, D.

2005; 13 (3): 423–82

- **A comparison between strand spaces and multiset rewriting for security protocol analysis** *JOURNAL OF COMPUTER SECURITY*
  Cervesato, I., Durgin, N. A., Lincoln, P. D., Mitchell, J. C., Scedrov, A.
  2005; 13 (2): 265–316
- **Probabilistic Polynomial-Time Semantics for a Protocol Security Logic.**
  Datta, A., Derek, A., Mitchell, John, C., Shmatikov, V., Turuani, M.
  2005
- **A modular correctness proof of IEEE 802.11i and TLS.**
  He, C., Sundararajan, M., Datta, A., Derek, A., Mitchell, John, C.
  2005
- **A derivation system and compositional logic for security protocols.** *Journal of Computer Security*
  Datta, A., Derek, A., Mitchell, John, C., Pavlovic, D.
  2005; 3 (13): 423-482
- **Security analysis of network protocols: logical and computational methods.**
  Mitchell, John, C.
  2005
- **Compositional Analysis of Contract Signing Protocols.**
  Backes, M., Datta, A., Derek, A., Mitchell, John, C., Turuani, M.
  2005
- **Games and the Impossibility of Realizable Ideal Functionality.** *IACR Cryptology ePrint Archive*
  Datta, A., Derek, A., Mitchell, John, C., Ramanathan, A., Scedrov, A.
  2005: 211
- **Security Analysis and Improvements for IEEE 802.11i.**
  He, C., Mitchell, John, C.
  2005
- **On the Relationships Between Notions of Simulation-Based Security.**
  Datta, A., Küsters, R., Mitchell, John, C., Ramanathan, A.
  2005
- **Enterprise privacy promises and enforcement.**
  Barth, A., Mitchell, John, C.
  2005
- **Proceedings of the 2005 ACM workshop on Formal methods in security engineering**
  edited by Atluri, V., Samarati, P., Küsters, R.
  2005
- **Multiset rewriting and the complexity of bounded security protocols.** *Journal of Computer Security*
  Durgin, Nancy, A., Lincoln, P., Mitchell, John, C.
  2004; 2 (12): 247-311
- **Client-Side Defense Against Web-Based Identity Theft.**
  Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, John, C.
  2004
- **A Distributed High Assurance Reference Monitor.**
  Chander, A., Dean, D., Mitchell, John, C.
  2004
- **Probabilistic Bisimulation and Equivalence for Security Analysis of Network Protocols.**
  Ramanathan, A., Mitchell, John, C., Scedrov, A., Teague, V.

2004

- **Reconstructing Trust Management.** *Journal of Computer Security*
  Chander, A., Dean, D., Mitchell, John, C.
  2004; 1 (12): 131-164
- **Analysis of the 802.11i 4-way handshake.**
  He, C., Mitchell, John, C.
  2004
- **Conflict and combination in privacy policy languages.**
  Barth, A., Mitchell, John, C., Rosenstein, J.
  2004
- **Securing Java RMI-Based Distributed Applications.**
  Li, N., Mitchell, John, C., Tong, D.
  2004
- **Abstraction and Refinement in Protocol Derivation.**
  Datta, A., Derek, A., Mitchell, John, C., Pavlovic, D.
  2004
- **Development of investigational radiation modifiers** *JOURNAL OF THE NATIONAL CANCER INSTITUTE*
  Colevas, A. D., Brown, J. M., Hahn, S., Mitchell, J., Camphausen, K., Coleman, C. N.
  2003; 95 (9): 646-651
- **A type system for the Java bytecode language and verifier** *JOURNAL OF AUTOMATED REASONING*
  Freund, S. N., Mitchell, J. C.
  2003; 30 (3-4): 271-321
- **Distributed Credential Chain Discovery in Trust Management.** *Journal of Computer Security*
  Li, N., Winsborough, William, H., Mitchell, John, C.
  2003; 1 (11): 35-86
- **A Derivation System for Security Protocols and its Logical Formalization.**
  Datta, A., Derek, A., Mitchell, John, C., Pavlovic, D.
  2003
- **Understanding SPKI/SDSI Using First-Order Logic.**
  Li, N., Mitchell, John, C.
  2003
- **Beyond Proof-of-Compliance: Safety and Availability Analysis in Trust Management.**
  Li, N., Winsborough, William, H., Mitchell, John, C.
  2003
- **Concepts in programming languages.**
  Mitchell, John, C.
  Cambridge University Press.2003
- **Security by typing.** *STTT*
  Debbabi, M., Durgin, Nancy, A., Mejri, M., Mitchell, John, C.
  2003; 4 (4): 472-495
- **Contract Signing, Optimism, and Advantage.**
  Chadha, R., Mitchell, John, C., Scedrov, A., Shmatikov, V.
  2003
- **Specifying and Verifying Hardware for Tamper-Resistant Software.**
  Lie, D., Mitchell, John, C., Thekkath, Chandramohan, A., Horowitz, M.

2003

- **DATALOG with Constraints: A Foundation for Trust Management Languages.**
  Li, N., Mitchell, John, C.
  2003
- **Secure protocol composition.**
  Datta, A., Derek, A., Mitchell, John, C., Pavlovic, D.
  2003
- **A Role-based Trust-management Framework.**
  Li, N., Mitchell, John, C.
  2003
- **Composition of Cryptographic Protocols in a Probabilistic Polynomial-Time Process Calculus.**
  Mateus, P., Mitchell, John, C., Scedrov, A.
  2003
- **Relating cryptography and formal methods: a panel.**
  Backes, M., Meadows, C., Mitchell, John, C.
  2003
- **A Compositional Logic for Proving Security Properties of Protocols.** *Journal of Computer Security*
  Durgin, Nancy, A., Mitchell, John, C., Pavlovic, D.
  2003; 4 (11): 677-722
- **Finite-state analysis of two contract signing protocols** *THEORETICAL COMPUTER SCIENCE*
  Shmatikov, V., Mitchell, J. C.
  2002; 283 (2): 419-450
- **Autonomous Nodes and Distributed Mechanisms.**
  Mitchell, John, C., Teague, V.
  2002
- **Multiset rewriting and security protocol analysis** *REWRITING TECHNIQUES AND APPLICATIONS*
  Mitchell, J. C.
  2002; 2378: 19-22
- **Design of a Role-Based Trust-Management Framework.**
  Li, N., Mitchell, John, C., Winsborough, William, H.
  2002
- **A Comparison between Strand Spaces and Multiset Rewriting for Security Protocol Analysis.**
  Cervesato, I., Durgin, Nancy, A., Lincoln, P., Mitchell, John, C., Scedrov, A.
  2002
- **Multiset Rewriting and Security Protocol Analysis.**
  Mitchell, John, C.
  2002
- **Programming language methods in computer security** *28th ACM/SIGPLAN/SIGACT Symposium on Principles of Programming Languages (POPL 2001)*
  Mitchell, J. C.
  ASSOC COMPUTING MACHINERY.2001: 1–3
- **A Probabilistic Polynomial-time Calculus For Analysis of Cryptographic Protocols (Preliminary Report).** *Electr. Notes Theor. Comput. Sci.*
  Mitchell, John, C., Ramanathan, A., Scedrov, A., Teague, V.
  2001; 45: 280-310
- **Distributed credential chain discovery in trust management: extended abstract.**
  Li, N., Winsborough, William, H., Mitchell, John, C.

2001

- **Programming language methods in computer security.**
  Mitchell, John, C.
  2001
- **Probabilistic Polynominal-Time Process Calculus and Security Protocol Analysis.**
  Mitchell, John, C., Ramanathan, A., Scedrov, A., Teague, V.
  2001
- **Probabilistic Polynomial-Time Process Calculus and Security Protocol Analysis.**
  Mitchell, John, C.
  2001
- **A Compositional Logic for Protocol Correctness.**
  Durgin, Nancy, A., Mitchell, John, C., Pavlovic, D.
  2001
- **A State-Transition Model of Trust Management and Access Control.**
  Chander, A., Mitchell, John, C., Dean, D.
  2001
- **Architectural support for copy and tamper resistant software** *9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS_IX)*
  Lie, D., Thekkath, C., Mitchell, M., Lincoln, P., Boneh, D., Mitchell, J., Horowitz, M.
  ASSOC COMPUTING MACHINERY.2000: 168–77
- **Analysis of Abuse-Free Contract Signing.** *Financial Cryptography*
  Shmatikov, V., Mitchell, John, C.
  2000
- **Analysis of a Fair Exchange Protocol.**
  Shmatikov, V., Mitchell, John, C.
  2000
- **Relating Strands and Multiset Rewriting for Security Protocol Analysis.**
  Cervesato, I., Durgin, Nancy, A., Mitchell, John, C., Lincoln, P., Scedrov, A.
  2000
- **A type system for object initialization in the Java bytecode language** *ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS*
  Freund, S. N., Mitchell, J. C.
  1999; 21 (6): 1196-1250
- **A formal framework for the Java bytecode language and verifier** *ACM SIGPLAN NOTICES*
  Freund, S. N., Mitchell, J. C.
  1999; 34 (10): 147-166
- **Optimization complexity of linear logic proof games** *Linear Logic 96 Tokyo Meeting*
  Lincoln, P. D., Mitchell, J. C., Scedrov, A.
  ELSEVIER SCIENCE BV.1999: 299–331
- **Parametricity and variants of Girard's J operator** *INFORMATION PROCESSING LETTERS*
  Harper, R., Mitchell, J. C.
  1999; 70 (1): 1-5
- **Probabilistic Polynomial-Time Equivalence and Security Analysis.**
  Lincoln, P., Mitchell, John, C., Mitchell, M., Scedrov, A.
  1999
- **A Meta-Notation for Protocol Analysis.**
  Cervesato, I., Durgin, Nancy, A., Lincoln, P., Mitchell, John, C., Scedrov, A.

1999

- **The type system for object initializatiion in the Jave bytecode language.** *ACM Trans. Program. Lang. Syst.*
  Freund, Stephen, N., Mitchell, John, C.
  1999; 6 (21): 1196-1250
- **A Formal Framework for the Java Bytecode Language and Verifier.**
  Freund, Stephen, N., Mitchell, John, C.
  1999
- **A Core Calculus of Classes and Objects.** *Electr. Notes Theor. Comput. Sci.*
  Bono, V., Mitchell, John, C., Patel, A., Shmatikov, V.
  1999; 20: 28-49
- **A type system for object initialization in the Java (TM) bytecode language** *ACM SIGPLAN NOTICES*
  Freund, S. N., Mitchell, J. C.
  1998; 33 (10): 310-328
- **On the relationship between classes, objects, and data abstraction** *3rd Workshop on Foundations of Object-Oriented Languages*
  Fisher, K., Mitchell, J. C.
  JOHN WILEY & SONS INC.1998: 3–25
- **A Probabilistic Poly-Time Framework for Protocol Analysis.**
  Lincoln, P., Mitchell, John, C., Mitchell, M., Scedrov, A.
  1998
- **A Type System for Object Initialization in the Java Bytecode Language.**
  Freund, Stephen, N., Mitchell, John, C.
  1998
- **Finite-State Analysis of Security Protocols.**
  Mitchell, John, C.
  1998
- **A Linguistic Characterization of Bounded Oracle Computation and Probabilistic Polynomial Time.**
  Mitchell, John, C., Mitchell, M., Scedrov, A.
  1998
- **Adding type parameterization to the Java(TM) language** *1997 ACM SIGPLAN Conference on Object-Oriented Programming Systems, Languages and Applications (OOPSLA 97)*
  Agesen, O., Freund, S. N., Mitchell, J. C.
  ASSOC COMPUTING MACHINERY.1997: 49–65
- **ML and beyond** *Programming Languages Workshop of the Strategic Directions in Computing Research*
  Harper, R., Mitchell, J. C.
  ASSOC COMPUTING MACHINERY.1997: 80–85
- **Adding Type Parameterization to the Java Language.**
  Agesen, O., Freund, Stephen, N., Mitchell, John, C.
  1997
- **Automated analysis of cryptographic protocols using Mur-phi.**
  Mitchell, John, C., Mitchell, M., Stern, U.
  1997
- **The analysis of programming structure.** *SIGACT News*
  Mitchell, John, C., Riecke, Jon, G.
  1997; 2 (28): 24-31
- **A Type System For Object Initialization In the Java Bytecode Language.** *Electr. Notes Theor. Comput. Sci.*
  Freund, Stephen, N., Mitchell, John, C.

1997; 10: 242-245

- **Strategic directions in software engineering and programming languages** *ACM COMPUTING SURVEYS*
  Gunter, C., Mitchell, J., Notkin, D.
  1996; 28 (4): 727-737
- **Standard ML-NJ weak polymorphism and imperative constructs** *8TH ANNUAL IEEE SYMP ON LOGIC IN COMPUTER SCIENCE (LICS 93)*
  Mitchell, J., Viswanathan, R.
  ACADEMIC PRESS INC ELSEVIER SCIENCE.1996: 102–16
- **Linear logic proof games and optimization.** *Bulletin of Symbolic Logic*
  Lincoln, P., Mitchell, John, C., Scedrov, A.
  1996; 3 (2): 322-338
- **The Complexity of Local Proof Search in Linear Logic.** *Electr. Notes Theor. Comput. Sci.*
  Lincoln, P., Mitchell, John, C., Scedrov, A.
  1996; 3: 120-129
- **ML and Beyond.** *ACM Comput. Surv.*
  Harper, R., Mitchell, John, C.
  1996; 4es (28): 219
- **Effective Models of Polymorphism, Subtyping and Recursion (Extended Abstract).**
  Mitchell, John, C., Viswanathan, R.
  1996
- **Foundations for programming languages.**
  Mitchell, John, C.
  Foundation of computing series, MIT Press.1996
- **The Development of Type Systems for Object-Oriented Languages.** *TAPOS*
  Fisher, K., Mitchell, John, C.
  1995; 3 (1): 189-220
- **Lower Bounds on Type Inference with Subtypes.**
  Hoang, M., Mitchell, John, C.
  1995
- **A Delegation-based Object Calculus with Subtying.**
  Fisher, K., Mitchell, John, C.
  1995
- **POLYMORPHISM AND SUBTYPING IN INTERFACES** *Workshop on Interface Definition Languages/1994 ACM Symposium on Principles of Programming Languages*
  Katiyar, D., LUCKHAM, D., Mitchell, J., Meldal, S.
  ASSOC COMPUTING MACHINERY.1994: 22–34
- **AN EXTENSION OF SYSTEM-F WITH SUBTYPING** *1st International Conference on Theoretical Aspects of Computer Software (TACS 91)*
  Cardelli, L., Martini, S., Mitchell, J. C., Scedrov, A.
  ACADEMIC PRESS INC JNL-COMP SUBSCRIPTIONS.1994: 4–56
- **Polymorphism and Subtyping in Interfaces.**
  Katiyar, D., Luckham, David, C., Mitchell, John, C.
  1994
- **A Type System for Prototyping Languages.**
  Katiyar, D., Luckham, David, C., Mitchell, John, C.
  1994
- **A lambda Calculus of Objects and Method Specialization.** *Nord. J. Comput.*
  Fisher, K., Honsell, F., Mitchell, John, C.

1994; 1 (1): 3-37

- **An Extension of System F with Subtyping.** *Inf. Comput.*
  Cardelli, L., Martini, S., Mitchell, John, C., Scedrov, A.
  1994; 1/2 (109): 4-56
- **Notes on Typed Object-Oriented Programming.**
  Fisher, K., Mitchell, John, C.
  1994
- **ON ABSTRACTION AND THE EXPRESSIVE POWER OF PROGRAMMING-LANGUAGES** *SCIENCE OF COMPUTER PROGRAMMING*
  Mitchell, J. C.
  1993; 21 (2): 141-163
- **ON THE TYPE-STRUCTURE OF STANDARD ML** *ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS*
  Harper, R., Mitchell, J. C.
  1993; 15 (2): 211-252
- **On Abstraction and the Expressive Power of Programming Languages.** *Sci. Comput. Program.*
  Mitchell, John, C.
  1993; 2 (21): 141-163
- **STANDARD ML-NJ WEAK POLYMORPHISM AND IMPERATIVE CONSTRUCTS** *8TH ANNUAL IEEE SYMP ON LOGIC IN COMPUTER SCIENCE (LICS 93)*
  Hoang, M., Mitchell, J., Viswanathan, R.
  I E E E, COMPUTER SOC PRESS.1993: 15–25
- **On the Type Structure of Standard ML.** *ACM Trans. Program. Lang. Syst.*
  Harper, R., Mitchell, John, C.
  1993; 2 (15): 211-252
- **Standard ML-NJ weak polymorphism and imperative constructs.**
  Hoang, M., Mitchell, John, C.
  1993
- **Type Inference with Extended Pattern Matching and Subtypes.** *Fundam. Inform.*
  Jategaonkar, L., Mitchell, John, C.
  1993; 1/2 (19): 127-165
- **A lambda calculus of objects and method specialization.**
  Mitchell, John, C., Honsell, F., Fisher, K.
  1993
- **DECISION-PROBLEMS FOR PROPOSITIONAL LINEAR LOGIC** *ANNALS OF PURE AND APPLIED LOGIC*
  Lincoln, P., Mitchell, J., Scedrov, A., Shankar, N.
  1992; 56 (1-3): 239-311
- **CONNECTING FORMAL SEMANTICS TO CONSTRUCTIVE INTUITIONS** *1991 SUMMER SYMP ON CONSTRUCTIVITY IN COMPUTER SCIENCE*
  Kurtz, S. A., Mitchell, J. C., Odonnell, M. J.
  SPRINGER VERLAG.1992: 1–21
- **OPERATIONAL ASPECTS OF LINEAR LAMBDA-CALCULUS** *7TH ANNUAL SYMP ON LOGIC IN COMPUTER SCIENCE (LICS 92)*
  Lincoln, P., Mitchell, J.
  I E E E, COMPUTER SOC PRESS.1992: 235–246
- **Algorithmic Aspects of Type Inference with Subtypes.**
  Lincoln, P., Mitchell, John, C.
  1992
- **Operational aspects of linear lambda calculus.**
  Lincoln, P., Mitchell, John, C.

1992

- **PER Models of Subtyping, Recursive Types and Higher-Order Polymorphism.**
  Bruce, Kim, B., Mitchell, John, C.
  1992
- **Notes on Sconing and Relators.**
  Mitchell, John, C., Scedrov, A.
  1992
- **Decision Problems for Propositional Linear Logic.** *Ann. Pure Appl. Logic*
  Lincoln, P., Mitchell, John, C.
  1992; 1-3 (56): 239-311
- **KRIPKE-STYLE MODELS FOR TYPED LAMBDA-CALCULUS** *2ND ANNUAL SYMP ON LOGIC IN COMPUTER SCIENCE*
  Mitchell, J. C., Moggi, E.
  ELSEVIER SCIENCE BV.1991: 99–124
- **ON ABSTRACTION AND THE EXPRESSIVE POWER OF PROGRAMMING-LANGUAGES** *LECTURE NOTES IN COMPUTER SCIENCE*
  Mitchell, J. C.
  1991; 526: 290-310
- **AN EXTENSION OF SYSTEM-F WITH SUBTYPING** *LECTURE NOTES IN COMPUTER SCIENCE*
  Cardelli, L., Martini, S., Mitchell, J. C., Scedrov, A.
  1991; 526: 750-770
- **An Extension of Standard ML Modules with Subtyping and Inheritance.**
  Mitchell, John, C., Meldal, S., Madhav, N.
  1991
- **Connecting Formal Semantics to Constructive Intuitions.**
  Kurtz, Stuart, A., Mitchell, John, C., O'Donnell, Michael, J.
  1991
- **Unification and ML-Type Reconstruction.** *Computational Logic - Essays in Honor of Alan Robinson*
  Kanellakis, Paris, C., Mairson, Harry, G., Mitchell, John, C.
  1991: 444–478
- **An Extension of System F with Subtyping.**
  Cardelli, L., Martini, S., Mitchell, John, C.
  1991
- **On Abstraction and the Expressive Power of Programming Languages.**
  Mitchell, John, C.
  1991
- **Type Inference With Simple Subtypes.** *J. Funct. Program.*
  Mitchell, John, C.
  1991; 3 (1): 245-285
- **Operations on Records.** *Mathematical Structures in Computer Science*
  Cardelli, L., Mitchell, John, C.
  1991; 1 (1): 3-48
- **Kripke-Style Models for Typed lambda Calculus.** *Ann. Pure Appl. Logic*
  Mitchell, John, C., Moggi, E.
  1991; 1-2 (51): 99-124
- **AN EXTENSION OF SYSTEM-F WITH SUBTYPING** *INTERNATIONAL CONF ON THEORETICAL ASPECTS OF COMPUTER SOFTWARE (TACS 91)*
  Cardelli, L., Martini, S., Mitchell, J. C., Scedrov, A.

SPRINGER-VERLAG BERLIN.1991: 750–770

- **THE SEMANTICS OF 2ND-ORDER LAMBDA CALCULUS** *INFORMATION AND COMPUTATION*
  Bruce, K. B., Meyer, A. R., Mitchell, J. C.
  1990; 85 (1): 76-134
- **OPERATIONS ON RECORDS** *5TH INTERNATIONAL CONF ON MATHEMATICAL FOUNDATIONS OF PROGRAMMING SEMANTICS*
  Cardelli, L., Mitchell, J. C.
  SPRINGER-VERLAG BERLIN.1990: 22–52
- **TOWARD A TYPED FOUNDATION FOR METHOD SPECIALIZATION AND INHERITANCE**
  MITCHELL, J. C., ASSOC COMP MACHINERY
  ASSOC COMPUTING MACHINERY.1990: 109–24
- **DECISION-PROBLEMS FOR PROPOSITIONAL LINEAR LOGIC** *31ST ANNUAL SYMP ON FOUNDATIONS OF COMPUTER SCIENCE*
  Lincoln, P., Mitchell, J., Scedrov, A., Shankar, N.
  I E E E, COMPUTER SOC PRESS.1990: 662–671
- **HIGHER-ORDER MODULES AND THE PHASE DISTINCTION** *17TH ANNUAL SYMP OF THE ASSOC FOR COMPUTING MACHINERY : PRINCIPLES OF PROGRAMMING LANGUAGES*
  Harper, R., Mitchell, J. C., Moggi, E.
  ASSOC COMPUTING MACHINERY.1990: 341–354
- **Higher-Order Modules and the Phase Distinction.**
  Harper, R., Mitchell, John, C., Moggi, E.
  1990
- **Decision Problems for Propositional Linear Logic.**
  Lincoln, P., Mitchell, John, C., Scedrov, A., Shankar, N.
  1990
- **Type Systems for Programming Languages.** *Handbook of Theoretical Computer Science, Volume B: Formal Models and Sematics (B)*
  Mitchell, John, C.
  1990: 365-458
- **Toward a Typed Foundation for Method Specialization and Inheritance.**
  Mitchell, John, C.
  1990
- **Operational and Axiomatic Semantics of PCF.**
  Howard, Brian, T., Mitchell, John, C.
  1990
- **The Semantics of Second-Order Lambda Calculus.** *Inf. Comput.*
  Bruce, Kim, B., Meyer, Albert, R., Mitchell, John, C.
  1990; 1 (85): 76-134
- **OPERATIONS ON RECORDS** *LECTURE NOTES IN COMPUTER SCIENCE*
  Cardelli, L., Mitchell, J. C.
  1989; 389: 75-81
- **Operations on Records.**
  Cardelli, L., Mitchell, John, C.
  1989
- **F-Bounded Polymorphism for Object-Oriented Programming.**
  Canning, Peter, S., Cook, William, R., Hill, Walter, L., Olthoff, Walter, G., Mitchell, John, C.
  1989
- **Polymorphic Unification and ML Typing.**
  Kanellakis, Paris, C., Mitchell, John, C.

1989

- **Operations in Records.**
  Cardelli, L., Mitchell, John, C.
  1989
- **ABSTRACT TYPES HAVE EXISTENTIAL TYPE** *ACM TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS*
  Mitchell, J. C., Plotkin, G. D.
  1988; 10 (3): 470-502
- **Polymorphic Type Inference and Containment.** *Inf. Comput.*
  Mitchell, John, C.
  1988; 2/3 (76): 211-249
- **ML with Extended Pattern Matching and Subtypes.**
  Jategaonkar, L., Mitchell, John, C.
  1988
- **The Essence of ML.**
  Mitchell, John, C., Harper, R.
  1988
- **Empty Types in Polymorphic Lambda Calculus.**
  Meyer, Albert, R., Mitchell, John, C., Moggi, E., Statman, R.
  1987
- **Kripke-Style models for typed lambda calculus.**
  Mitchell, John, C., Moggi, E.
  1987
- **Representation Independence and Data Abstraction.**
  Mitchell, John, C.
  1986
- **Realisability Semantics for Error-Tolerant Logics.**
  Mitchell, John, C., O'Donnell, Michael, J.
  1986
- **A Type-Inference Approach to Reduction Properties and Semantics of Polymorphic Expressions (Summary).**
  Mitchell, John, C.
  1986
- **Second-Order Logical Relations (Extended Abstract).**
  Mitchell, John, C., Meyer, Albert, R.
  1985
- **Abstract Types Have Existential Type.**
  Mitchell, John, C., Plotkin, Gordon, D.
  1985
- **Semantic Models for Second-Order Lambda Calculus.**
  Mitchell, John, C.
  1984
- **Coercion and Type Inference.**
  Mitchell, John, C.
  1984
- **On the Sequential Nature of Unification.** *J. Log. Program.*
  Dwork, C., Kanellakis, Paris, C., Mitchell, John, C.

1984; 1 (1): 35-50

- **The Implication Problem for Functional and Inclusion Dependencies.** *Information and Control*
  Mitchell, John, C.
  1983; 3 (56): 154-173
- **Termination Assertions for Recursive Programs: Completeness and Axiomatic Definability.** *Information and Control*
  Meyer, Albert, R., Mitchell, John, C.
  1983; 1/2 (56): 112-138
- **Inference Rules for Functional and Inclusion Dependencies.**
  Mitchell, John, C.
  1983
- **Axiomatic Definability and Completeness for Recursive Programs.**
  Meyer, Albert, R., Mitchell, John, C.
  1982