Curriculum Vitae
Raj Katti

Interests

Current Interests: Cryptography, Digital Systems.
Past Interests: Data Compression, Computer Architecture, Error Correcting Codes, Computer Arithmetic, Fault Tolerant Computing.

Academic Background

Ph.D., School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA, 1991.
M.S., School of Electrical Engineering and Computer Science, Washington State University, Pullman, WA, 1987.
M.S., Mechanical Engineering, University of Idaho, Moscow, Idaho, 1985.
B. Tech., Mechanical Engineering, Indian Institute of Technology, Bombay, India, 1983.

Academic Experience/Employment History

July 2015-present: Interim Director, Institute of Technology, UW Tacoma.
June 2014-June 2015: Professor, Institute of Technology, University of Washington Tacoma.
August 2011-13: Interim Chair, Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58108
August 2006-2014: Professor (Tenured), Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58108
August 2001-2006: Associate Professor (Tenured), Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58108
July 2000-July 2001: Senior Design Engineer, Intel Architecture Group, Intel Corporation, Hillsboro, Oregon.
August 2001-Dec. 2002: Co-director, Sensor Electronics Group, Center for NanoScale Science and Engineering (CNSE), North Dakota State University.
August 1999-August 2000: Associate Professor with Tenure, Department of Electrical and Computer Engineering, North Dakota State University.
August 1998-August 1999: Associate Professor, Department of Electrical and Computer Engineering, Wichita State University, Wichita, Kansas.
August 1997-August 1998: Associate Professor with Tenure, Department of Electrical and Computer Engineering, North Dakota State University.
August 1991-August 1997: Assistant Professor, Department of Electrical and Computer Engineering, North Dakota State University.

Teaching, Advising, and Curriculum Development

Summary

- Goal: to maintain rigor in my courses and foster enthusiasm in learning.
- Research and teaching go hand-in-hand. Ideas obtained in the classroom lead to new research ideas and new discoveries are presented in the classroom to improve my teaching.
- Use my industry experience at Intel to motivate students and improve my quality of instruction via real world examples.
- Developed cutting edge courses like, Digital Systems Testing and Hardware for Cryptography.

Courses taught and student ratings

University of Washington Tacoma:
Courses Taught:
Digital Systems (TCES 230), Electronics (TCES 312), Intro to Computer Engineering (TCES 101 &102), Theory of Computing (TCSS 540), Algorithms (TCSS 343), Network Security (TCSS 431).

Student Rating: Mostly above 4 out of 5.

Curriculum Development: Developed a new course in Hardware for Cryptography.

Graduate Students: Advised one MSCSS student (Shruti More).

NDSU:
Undergraduate Courses:
Cryptographic Protocols (ECE 494), Microcomputer Interfacing (ECE 376), Digital systems testing (ECE 470), Digital Systems (ECE 275), VHDL (ECE 375), Assembly Language Programming (ECE 373), C++ (ECE 173), Fault Tolerant Computing (ECE 470), Digital Electronics (ECE 423), Data Structures.

Graduate Courses:
Cryptographic Protocol Theory (ECE 796), Computer Architecture (ECE 774), Digital Electronics (ECE 623), Hardware for Cryptography (ECE 775), Information Theory (ECE 745).

Student Rating:
I am consistently rated between 3.5 and 4.8 out of 5 in all the courses I have taught.

Curriculum development

1. Developed the Computer Engineering Curriculum for the new Bachelors degree in Computer Engineering. I now lead the effort in improving all aspects of the computer engineering program at NDSU.
2. I have incorporated real life examples from my experience at Intel into my courses. The students have consistently remarked that this has given them a new perspective on the course material.
3. I have developed five new courses in the ECE department. These are "ECE 494 Cryptographic Protocols", "ECE 470 Digital Systems Testing", "Information Theory", "Cryptographic Protocol Theory," and "ECE 775 Hardware for Cryptography". In these courses I give examples of my work at Intel.

Educational Committees

I have been a member of the Department of ECE curriculum and assessment committees. These committees assess our courses and curricula and make recommendations on changes that need to be made for improvement.

Advising

1. I am the academic advisor for 30 Undergraduate students. Typically I meet with each student 2 to 3 times every semester. The advice given is mainly on course work and their curriculum.
2. I was the advisor for the IEEE student branch. I met with the office bearers once a month and the number of student members were around 100. The advice mainly consisted of finding speakers for the monthly seminar, helping incoming freshmen with course work, providing help with selecting electives etc.

Graduate Students

In the recent past I have been the major professor for the following graduate students:

	Name	Year Graduating	Degree	Thesis title
1.	A. Mamun	2004	M.S.	Low Power LFSR Design
2.	Y. Pawar	Fall 2005	M.S.	CAN Networks for Automobiles
3.	B. Xiaoyu	Fall 2005	M.S.	Implementing Adders with Signed Digit numbers
4.	D. Rautela	2006	M.S.	Routing algorithms for FPGAs
5.	H. Khattri	2007	M.S.	Performance of Wireless Networks
6.	M. Dangol	2007	M.S.	Using Arithmetic codes for Encryption
7.	X. Ruan	2005	M.S.	Test Vector Compression for Systems on a Chip
8.	G. Ravindran	2007	M.S.	Implementation of LDPC codes
9.	A. Mamun	2007	Ph.D	Design of Novel A/D and D/A converters
10.	K. Mangipudi	2006	Ph.D	Authentication Protocols with User

				Anonymity
11.	X. Ruan	2007	Ph.D	Signed binary recoding for Elliptic curve cryptography
12.	Vyasa Sai	2008	M.S.	Secure pseudo-random bit sequence generation
13.	Ahana Ghosh	2009	M.S.	Using data compression for encryption
14.	Revathi Dhamotharan	2012	M.S.	Efficient generation of Message Authentication Codes Using Polynomial Division
15.	Aida Vosoughi	2011	M.S.	On the security of multimedia encryption and authentication schemes.
16.	Rucha Sule	2013	M.S.	Authentication in the Smart-Grid
17.	Sarjan Shrestha	2013	M.S.	Quantum Dot Automata
18.	Akshaya Mohan	2013	M.S.	Provable Data Possession
19.	Sayantica Pattanayak	2015	M.S.	Efficient Attributes for Secure Credentials using the Chinese Remainder Theorem
20.	Gerardo Zamora	2015	M.S.	Hardware Implementation of the Multiplication Protocol
21.	Abdul Hameed	2015	Ph.D.	Improving Video Perception
22.	Nauman Jalil	2015	Ph.D.	Cryptographic hardware
23.	Raja Ali Riaz	2016	Ph.D.	Cryptographic protocols

Graduate Committee Member

I have been/am a committee member on several students' graduate committee. These students were/are in the ECE department, other engineering departments, mathematics and computer science departments.

Senior design projects

I usually advise one senior design group (three students) per year. This involves coming up with a project and then overseeing their progress through out the year via weekly meetings. In 2001-02 I took on a larger load and advised 3 senior design projects.

Undergraduate research

I advised one senior (David Hinkemeyer) who was part of my group associated with the NSF grant. I received the NSF REU (research experience for undergraduates) grant to fund him on his research activities. David attended graduate school at the University of Wisconsin.

I also advised a "scholar team" (a group of undergraduates) for conducting research in the field of cryptography.

Personal and professional development to improve teaching effectiveness

- In the year 2000-01 I went on leave without pay to work for Intel. This experience has helped me in both my research and teaching. My courses now incorporate a lot of

examples that have come out of my Intel experience and Intel has funded a research project on wireless networks.

- Attended a workshop on teaching methods at NDSU in 2001.

Research, Creative, and Professional Activities

Summary

- Goal: to spread the joy of discovery to students and other faculty members via rigorous teaching and research.
- Research and teaching go hand-in-hand. Ideas obtained in the classroom lead to new research ideas and new discoveries are presented in the classroom to improve my teaching.
- Maintaining a high quality of research is very important to me and evidence of this is seen by my publications in top journals and conferences and funding from NSF and the Intel Corporation.
- In all my work I am the person who has provided the central idea and part of the work has been carried out by my graduate students. I am the principle investigator in all my funded work.

Publications

Refereed Journal Publications

1. Aida Vosoughi, Raj Katti, and Rucha Sule, "Fast Message Authentication Code for Multiple Messages with Provable Security," to be submitted to the *IEEE Transactions on Computers*, 2013.
2. Raj S. Katti and Aida Vosoughi, "On the Security of Key-based Interval Splitting Arithmetic Coding with respect to Message Indistinguishability," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 3, pp. 895-903, June 2012.
3. Raj S. Katti, Sudarshan Srinivasan, and Aida Vosoughi, "On the Security of Randomized Arithmetic Codes against Ciphertext-only Attacks," *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 1., pp. 19-27, March 2011.
4. Rajendra Katti and Sudarshan Srinivasan, "Sub-optimal data compression and the subset sum problem," *AEU-International Journal of Electronics and Communications*, Vol. 65, Issue 1, pp. 53-61, Jan. 2011.
5. Rajendra Katti and Rajesh Kavasseri, "Nonce Generation for the Digital Signature Standard," *International Journal of Network Security*, Vol. 11, No. 1, pp. 23-32, July 2010. 2 citations.
6. Rajendra Katti, Rajesh Kavasseri and Vyasa Sai, " Pseudorandom bit generation using coupled congruential generators," The *IEEE Transactions on Circuits and Systems—II: Express Briefs*, Vol. 57, No. 3, Mar. 2010.
7. Sudarshan Srinivasan, K. Sarkar and Rajendra Katti, " Verification of Synchronous elastic Processors," *IEEE Embedded Systems Letters*, Vol. 1, No. 1, pp. 14-18, Sept. 2009.
8. Sudarshan Srinivasan, K. Sarkar and Rajendra Katti, " Token-Aware Completion functions for Elastic Processor Verification," *Research Letters in Electronics*, Vol. 2009, Article ID 480740, 5 pages, 2009.

9. Rajendra Katti and Joseph Brennan, “Montgomery Multiplication over Rings,” *Journal of the Franklin Institute*, Vol. 346, No. 1, pp. 10-16, Feb. 2009.
10. Xiaoyu Ruan and Rajendra Katti, “Data-Independent Pattern Run-Length Compression for Testing Embedded Cores in SoCs,” *The IEEE Transactions on Computers*, Vol. 56, No. 4, pp545-556, April 2007. 9 citations.
11. Kumar Mangipudi and Rajendra Katti, "A Secure Identification and Key agreement protocol with user Anonymity (SIKA)", *Elsevier Computers and Security*, Vol. 25, pp. 420-425, 2006. 11 citations.
12. Xiaoyu Ruan and Rajendra Katti, “A New Source Coding Scheme with small Expected Length and Its Application to Simple Data Encryption,” *The IEEE Transactions on Computers*, Vol. 55, No. 10, pp 1300-1305, Oct. 2006. 4 citations.
13. Kumar Mangipudi, Rajendra Katti, and Huirong Fu, “Authentication and Key Agreement Protocols with User Anonymity,” *The International Journal of Network Security*, Vol. 3, No. 3, pp 259-270, Nov. 2006. 13 citations.
14. Kumar Mangipudi and Rajendra Katti, “A Hash-Based Strong Password Authentication Protocol with User Anonymity,” *The International Journal of Network Security*, Volume: 2, No: 3 (May 1, 2006), pp. 225-229. 13 citations.
15. Rajendra Katti, Xiaoyu Ruan, and Hareesh Khattri, “Multiple-Output Low-Power Linear Feedback Shift Register Design,” *The IEEE Transactions on Circuits and Systems*, Vol. 53, No. 7, pp 1487-1495, July 2006. 2 citations.
16. Clemens Heuberger, Rajendra Katti, Helmut Prodinger, and Xiaoyu Ruan, “The Alternating Greedy Expansion and Applications to Computing Digit Expansions from Left-to-Right in Cryptography”, *Theoretical Computer Science*, a publication of European Association for Theoretical Computer Science (EATCS) and Elsevier Science Publishers, Volume 341, Issues 1-3, 5 September 2005, Pages 55-72. 19 citations.
17. X. Ruan and Rajendra Katti, “Left-to-Right Optimal Signed-Binary Representation of a Pair of integers,” *The IEEE Transactions on Computers*, Vol. 54, No. 2, pp. 132-140, Feb. 2005. 21 citations.
18. Rajendra Katti and J. Brennan, “Low Complexity Multiplication in a finite field using ring representation,” *The IEEE Transactions on Computers*, Special Section on Cryptographic Hardware and Embedded Systems, Guest Editors, C. K. Koc and C. Paar, pp. 418-427, April 2003. 20 citations.
19. Rajendra Katti, “Test Pattern Generation and signature analysis for burst errors,” *The IEEE Transactions on Circuits and Systems II*, Vol. 45, No. 3, pp 410-414, March 1998.
20. Rajendra Katti and M. L. Manwaring, “Performance based design of high-level language-directed computer architectures,” *The IEEE Trans. On Systems, Man and Cybernetics*, Vol. 28, No. 2, pp219-226, April 1998.
21. Rajendra Katti, “Non-prime memory systems and error correction in address translation,” *The IEEE Transactions on Computers*, Vol. 46, No. 1, pp 75-79, Jan. 1997. 2 citations.
22. Rajendra Katti and Mario Blaum, “An Improvement on the construction of t-EC/AUED codes,” *The IEEE Transactions on Computers*, Vol. 45, No. 5, pp 607-609, May 1996. 9 citations.

23. Rajendra Katti, "A New Residue Arithmetic Error Correction Scheme," *The IEEE Transactions on Computers*, Vol. 45, No. 1, pp 13-19, Jan. 1996. 14 citations.
24. Rajendra Katti, "A Note on SEC/AUED codes," *The IEEE Transactions on Computers*, Vol. 45, no. 2, pp 244-247, Feb. 1996. 4 citation.
25. Rajendra Katti, "Comments on, "A systematic (16,8) code for correcting double errors and detecting triple-adjacent errors."," *The IEEE Transactions on Computers*, Vol. 44, No.12, pp 1472-1473, Dec. 1995.
26. Rajendra Katti, "A Modified Booth Algorithm for high radix fixed-point multiplication," *The IEEE Transactions on VLSI systems*, Vol. 2, No. 4, pp 522-524, Dec.1994. 7 citations.
27. Rajendra Katti, "Comments on "Decomposition of complex multipliers using polynomial encoding"," *The IEEE Transactions on Computers*, Vol. 43, No. 3, pp 381-383, March 1994.
28. Rajendra Katti, R. T. Jacobsen, R. B. Stewart, and M. Jahangiri, "Thermodynamic Properties of Neon for Temperatures from the Triple Point to 700 K at Pressures to 700 Mpa,"*Advances in Cryogenic Engineering*, Vol. 31, pp 1189-1197, Plenum, New York, 1986.

Fully Refereed Conference Publications

1. "Efficient Unconditionally Secure Comparison and Private Preserving Machine Learning Classification Protocols," Bernardo David, Rafael Dowsley, Raj Katti and Anderson Nascimento, *The 9th International Conference on Provable Security*, Kanazawa, Japan, 2015.
2. Khot, Amruta, Abdeltawab Hendawi, Anderson Nascimento, Raj Katti, Ankur Teredesai, and Mohamed Ali. "Road network compression techniques in spatiotemporal embedded systems: A survey." In Proceedings of the 5th ACM SIGSPATIAL International Workshop on GeoStreaming, pp. 33-36. ACM, 2014.
3. S. More and Raj Katti, "Efficient generation of discrete Gaussian samples for low power applications in cryptography," 2015 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing.
4. S. Pourbaksh and Raj Katti, "Efficient Attributes for Secure Credentials," 2015 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing.
5. Rajendra Katti and Cristinel Ababei, "Secure Comparison without explicit XOR," Ninth European Dependable Computing Conference, Sibiu, Romania, 2012.
6. Rucha Sule, Rajendra Katti, and Rajesh Kavasseri, "A variable length fast message authentication code for secure communication in smardgrids," *2012 IEEE Power Engineering Society General Meeting*, July 2012.
7. Raj Katti and Sarjan Shrestha, "Novel Asynchronous registers for Sequential Circuits with Quantum-dot cellular automata," *IEEE International Symposium on Circuits and Systems*, pp. 1351-1354, May 2012.

8. Akshaya Mohan and Rajendra Katti, "Provable Data Possession Using Sigma-Protocols," *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*, June 2012.
9. Sudarshan Srinivasan and Raj Katti, "Desynchronization: Design for Verification," *Proceedings of the 11th Conference on Formal Methods in Computer Aided Design*, FMCAD 2011, pp. 215-222, 2011.
10. Aida Vosoughi and Rajendra Katti, "Fast Message Authentication Code for Multiple Messages with Provable Security," *Proceedings of the IEEE Global Communication Conference*, 2010, GLOBECOM 2010, Dec. 6-10, Miami, Florida.
11. Cristinel Ababei and Rajendra Katti, "Achieving network on chip fault tolerance by adaptive remapping," IPDPS, pp. 1-4, 2009. 2 citations.
12. Rajendra Katti and Sudarshan Srinivasan, "Efficient Hardware implementation of a new pseudo-random bit sequence generator." Invited Paper. *The IEEE International Symposium on Circuits and Systems*, Taipei, Taiwan, May 2009. 1 citation.
13. Rajendra Katti and Sudarshan Srinivasan, "Verification of desynchronized circuits." *The IEEE International Symposium on Circuits and Systems*, Taipei, Taiwan, May 2009. 1 citation.
14. Rajendra Katti and Ahana Ghosh, "Security using Shannon-Fano-Elias Codes." *The IEEE International Symposium on Circuits and Systems*, Taipei, Taiwan, May 2009.
15. Rajendra Katti, Kane Iverson, and John Vreugdenhil, "Image encryption using dynamic shuffling and XORing processes." *The IEEE International Symposium on Circuits and Systems*, Taipei, Taiwan, May 2009.
16. Rajendra Katti and Rajesh Kavasseri, "Secure Pseudo-random Bit Sequence Generation using Coupled Linear Congruential Generators," Proceedings of the *IEEE International Symposium on Circuits and Systems*, Seattle, WA, May 2008. 3 citations.
17. Xiaoyu Ruan and Rajendra Katti, "An Efficient Data Independent Technique for Compressing Test Vectors in Systems-on-a-Chip," *2006 IEEE International Symposium on VLSI*. 15 citations.
18. Xiaoyu Ruan and Rajendra Katti, "Using Improved Shannon-Fano-Elias Codes for Data Encryption," *2006 International Symposium on Information Theory*, pp 1249-1252.
19. Xiaoyu Ruan, Rajendra Katti, and David Hinkemeyer, "Algorithm and implementation of signed binary recoding with asymmetric digit sets for elliptic curve cryptosystems," Invited paper for the Special Session on New Generation Architectures/Implementations for Security Protocols & Cryptography Applications, *The International Symposium on Circuits and Systems*, Kos, Greece, 2006. 1 citation.
20. Hareesh Khattri and Rajendra Katti, "Implementation and performance analysis of IEEE 802.11i standard using the IXP425 Network processor," *2nd ACM Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks* (PE-WASUN' 2005), Montreal, Canada, Oct. 2005.
21. Xiaoyu Ruan and Rajendra Katti, "Cryptanalysis of the Shannon-Fano-Elias Code," *The International Symposium on Information Theory*, Adelaide, Australia, Sept. 2005.

22. Deepak Rautela and Rajendra Katti, "Design and Implementation of FPGA Router for Efficient Utilization of Heterogeneous Routing Resources," *The IEEE Computer Society's Annual Symposium on VLSI* (ISVLSI), pp 232-237, Tampa, Florida, May 2005. 8 citations.
23. Xiaoyu Ruan and Rajendra Katti, "Transmission-Service Pricing Based on Real-Time Power Network Conditions", accepted by 2005 *IEEE Power Engineering Society General Meeting*, June 12-16, 2005, San Francisco, CA.
24. Xiaoyu Ruan and Rajendra Katti, "On the Signed-Binary Window Method", accepted by 2005 *IEEE International Symposium on Circuits and Systems*, May 23-26, 2005, Kobe, Japan.
25. Rajendra Katti and Xiaoyu Ruan, "S-Code: New Distance-3 MDS Array Codes", accepted by 2005 *IEEE International Symposium on Circuits and Systems*, May 23-26, 2005, Kobe, Japan. 4 citations.
26. Rajendra Katti and Xiaoyu Ruan, "S-Code: New MDS Array Codes with Optimal Encoding", accepted by 2005 *IEEE International Conference on Acoustics, Speech, and Signal Processing*, March 18-23, 2005, Philadelphia, PA.
27. Deepak Rautela and Rajendra Katti, "Efficient Utilization of Heterogeneous Routing Resources for FPGAs," *International Symposium on Field Programmable Gate Arrays*, Monterey, CA, Feb. 20-22 2005.
28. Rajendra Katti, Xiaoyu Ruan, and Bing Xiao, "Signed Binary Addition Circuitry Based on Two-Bit Encoding Schemes", in proceedings of 2004 *International Symposium on Integrated Circuits, Devices and Systems*, September 8-10, 2004, Singapore.
29. Xiaoyu Ruan and Rajendra Katti, "Low-Weight Left-to-Right Binary Signed Digit Representation of N Integers", in proceedings of 2004 *IEEE International Symposium on Information Theory*, pp. 548, June 27-July 2, 2004, Chicago, IL.
30. Rajendra Katti and Xiaoyu Ruan, "Left-to-Right Binary Signed-Digit Recoding for Elliptic Curve Cryptography", in proceedings of 2004 *IEEE International Symposium on Circuits and Systems*, Volume 2, pp. 365-368, May 23-26, Vancouver, Canada. 4 citations.
31. Rajendra Katti and Abdullah Mamun, "Low Power Linear Feedback Shift Registers", in proceedings of 2004 *IEEE International Symposium on Circuits and Systems*, May 23-26, Vancouver, Canada. 4 citations.
32. Kumar Mangipudi, Nagaraja Malneedi, Rajendra Katti, and Huirong Fu, "Attacks and Solutions on Aydos-Savas-Koç's Wireless Authentication Protocol", Symposium on Network and Security management, *the IEEE Global Telecommunications Conference*, Nov 29-Dec 3, Dallas, TX 2004.
33. D. M. Schneider, C. M. Ripplinger, K. Gilbertson, Rajendra Katti, and M. J. Schroeder, "Optically-based control of a Prosthetic Device," 2003 *Summer Bioengineering Conference*, Key Biscayne, Florida, June 25 –29, 2003.

34. Rajendra Katti, "Speeding up Elliptic Curve Cryptosystems using a new signed Binary Representation for Integers," Proceedings of *the EuroMicro Symposium on Digital Systems Design*, DSD 2002, pp 380-383, September 2002. 16 citations.
35. Rajendra Katti and V. V. Bapeswara Rao, "An Array based technique for Routing Messages in Distributed Double Loop Networks," Proceedings of the 2002 *IEEE International Symposium on Circuits and Systems*, Phoenix, Arizona.
36. Rajendra Katti and Longfei Hu, "A Parallel Algorithm to solve Continuous Time Markov Processes that Model the Performance of Parallel Computers," *The 8th SIAM conference on Parallel Processing for Scientific Computing*, Nov. 1996.
37. Rajendra Katti and Huaan Zhang, "An Iterative Algorithm using Probabilistic Automata for predicting the Performance of Parallel Computers," *The 8th SIAM conference on Parallel Processing for Scientific Computing*, Nov. 1996.
38. Rajendra Katti and Longfei Hu, "On Linear skewing for parallel array access," *North Dakota Academy of Science*, 1995.
39. Rajendra Katti, "Performance analysis of parallel computations," Proceedings of *the International Conference on Parallel and Distributed Computing*, 1993.
40. Jenny Rawson and Rajendra Katti, "The iterative solution of Lyapunov Equations," *7th SIAM Conference on Parallel Processing for Scientific Computing and Systems*, pp 421-426, Oct. 1993.
41. Rajendra Katti, and M. L. Manwaring, "A Design Methodology for Language Directed Architectures," Accepted by *the 33rd Midwest Symposium on Circuits and Systems*, August 12-14, 1990.
42. M. F. Chowdhury, Rajendra Katti and M. L. Manwaring, "Design and Modeling of Real-time Systems," Accepted by *the 33rd Midwest Symposium on Circuits and Systems*, August 12-14, 1990.
43. Rajendra Katti and M. L. Manwaring, "Information Structures in Language Directed Architectures and their Design," *The International Conference on Computer Applications in Design, Simulation and Analysis*, March 1990.
44. Rajendra Katti and M. L. Manwaring, "Information Structures in Language Directed Architectures," *22nd Annual International Workshop on Microprogramming and Microarchitecture*, Dublin, Ireland, pp 122-127, August 1989.
45. Rajendra Katti and M. L. Manwaring, "Executing Sequential Programs in Parallel on a Multiprocessor Architecture," *Proceedings of the IEEE 3rd Annual Parallel Processing Symposium*, pp 385-400, March 1989.

Grants, Contracts, and Awards

Funded Proposals

1. Rajendra Katti and Sudarshan Srinivasan, Design of an Embedded Systems Laboratory, John Deere Corporation, $12,000 (approx.), 2011-2012.
2. Rajendra Katti and Ananda Shastri, Design of a first-year electronics lab manual for physics and engineering students that incorporates research-led teaching, Tri-College University Collaborative Grant, $1000, 2009-2010.
3. Rajendra Katti, K. E. Nygard, B. M. Slater, and C. I. Harter, Collaborative Scholarships in Computing, Information Sciences, and Engineering, *NSF*, $463,000, 2007-2011.

4. Rajendra Katti (PI), Optimal recoding of binary numbers for cryptographic operations, *NSF/REU*, $6250, 2005-2006.
5. Rajendra Katti (PI), Optimal recoding of binary numbers for cryptographic operations, *NSF*, $150,000, 2004-2007.
6. Rajendra Katti (PI), Speech Encryption for Wireless LAN, *INTEL Corporation*, $60,000, 2004-2007.
7. Rajendra Katti (PI), Equipment grant from Dean, College of Engineering, for development of a wireless network, $4096, 2005.
8. Rajendra Katti (PI), Equipment grant from *Intel Corporation*, $10,000, 2004-2005.
9. Rajendra Katti (PI), Equipment grant for VXWorks real time operating system from *WindRiver Corporation*, $100,000, 2004-2005.
10. Rajendra Katti (PI), "Cryptographic algorithms for Sensors," *Defence Military Electronics Agency*, $30,000, 2004.
11. Rajendra Katti (PI), "Secure Communication with Wireless Sensors," *Defence Military Electronics Agency*, $45,000, 2003.
12. Rajendra Katti (PI), "New cryptographic hardware for Network security applications," *NSF/EPSCOR*, $15,000, 2002-2003.
13. Rajendra Katti (co-PI, 50% responsibility) and Joel Jorgenson, "CNSE: Sensor Electronics Group Creation and Management," *Defence Military Electronics Agency*, $800,000, 2002-2004.
14. Rajendra Katti (PI), "Using the Chinese Remainder Theorem in Fault Tolerant Computing." *NSF/EPSCOR*, $15,000, 1996-1998.
15. Rajendra Katti (PI), "A Tool for the Performance Evaluation of Parallel Computers." *NSF/RIA*, $78,855, 1993-1997.
16. Rajendra Katti (co-PI, 50% responsibility) and Rawson, J., "Fast algorithms for solving the discrete time Ricatti Equations," *Grant-in-aid*, $4100, 1993.

<u>Applied for 3 patents:</u>

1. Abdullah Mamun and Rajendra Katti, Low-power Linear Feedback Shift Register, May 2005. I have provided the central idea in this patent.
2. Xiaoyu Ruan and Rajendra Katti, Recoding of binary numbers for cryptography, May 2005. I have provided the central idea in this patent.
3. Rajendra Katti and Rajesh Kavasseri, Secure Pseudo-random bit sequence generation using coupled linear congruential generators, Summer 2008. I have provided the central idea in this patent.

Service

Committee/University Involvement

University of Washington Tacoma:

1. Search Committee Member, 2014: two positions in CES, one position in security.
2. Search Committee Member, 2015: one position in CSS, four lecturer positions in CSS.
3. CES Curriculum Committee Chair: 2014-present.

North Dakota State University:

Department Level Involvement

1. ECE department Interim Chair: 2011-13.
2. ECE department PTE committee chair, 2010- 2011.
3. ECE department Chair search committee, 2010, member.
4. Member of the Department of ECE Promotion, Tenure and Evaluation Committee, 2005-present.
5. Faculty Mentor for new faculty members, 2005-2009.
6. Department of ECE Assessment Committee, 2001-present, member.
7. Department of ECE Graduate admission Committee, 2001-present, member.
8. Maintain License for Mentor Graphics Software for Department of ECE, 2001 to 2008.
9. Department of ECE Faculty Search Committee (for 3 positions), 2007-2008, Chair.
10. Department of ECE Faculty Search Committee, 2001-2002, Chair.
11. Department of ECE Faculty Search Committee, 2004-2005, member.
12. Advisor to the IEEE student branch, 1996-1997 and 1999-2000.
13. I developed the Computer Engineering curriculum for the department of ECE, 1998. Since then I have led all efforts to improve the computer engineering program.
14. Department of ECE Curriculum Committee, 1995-1997, member. The committee is responsible for making recommendations on the electrical engineering curriculum and on proposals on changing the curriculum.
15. Supervised the System Administrator, 1991-1992. The system administrator was a graduate student who maintained the HP9000 and HP64000 in the Department of Electrical Engineering.

College Level Involvement

1. Promotion, Tenure and Evaluation Committee, College of Engr. and Arch., 2007-08, 2010-present, member.
2. Academic Affairs Committee, College of Engr. and Arch., 2005-2009, member.
3. Public Relations Committee, College of Engr. and Arch, 2001 – 2006, member.
4. Research and Extension Committee, College of Engr. and Arch, 2003 – 2007, member.
5. Academic Affairs Committee, College of Engr. and Arch., 1994-1997, member.

University Level Involvement

1. Dean Smith Evaluation Committee, 2010, member.
2. Committee to improve graduate student disquisitions (ad hoc committee formed by Dean Wittrock), 2010, member.
3. Developed a collaboration for student and faculty exchange with the Indian Institute of Information Technology, Pune, India, 2007.
4. Reviewed proposals for the Research Administration Office at NDSU, 2005.
5. Co-director of Sensor Electronics Group, CNSE (Center for NanoScale Science and Engineering): performed personnel hiring, management of the group and gave presentations to companies visiting NDSU.
6. Member of an ad hoc committee appointed by the Dean of the Graduate School to improve quality of theses and dissertations, Sept. 2008 – March 2009.

Service to the Profession

1. Organized Reviews of 6 papers in the area of Cryptography for the 2011 IEEE International Symposium on Circuits and Systems.
2. Reviewer for the Computer Journal, and Computers and Security an Elsevier Journal, 2010.
3. Member of the Technical Program Committee for the following conferences. IEEE WCNIS 2010 (Communications and Information Security) and the 2009 IEEE International Conference on Vehicular Electronics and Safety.
4. Organized Reviews of 13 papers in the area of Cryptography for the 2010 IEEE International Symposium on Circuits and Systems.
5. Chair for the session on "Cryptographic Systems," The IEEE International Symposium on Circuits and Systems, May 2009.
6. Associate Editor, Journal of Circuits, Systems and Computers, World Scientific, 2004-2014.
7. Member of the Technical Committee on Communication in the IEEE Circuits and Systems Society. This committee organizes the Communication based research papers in the International Symposium on Circuits and Systems, 2003-Present.
8. Proposal reviewer for the NSF, 2003, 2005.
9. Organized Reviews of 30 papers for the 2003 IEEE International Symposium on Circuits and Systems.
10. Reviewer for two textbooks.
    - Dr. R. F. Tinder, Engineering Digital Design, Academic Press, 2000.
    - Dr. M. L. Manwaring and V. D. Malbasa, Engineering the Hardware-Software Interface, Prentice Hall, 2005.
11. Member of the Planning Committee that organized the 58th Annual ASEE North Midwest Section Meeting (Oct. 3-5, 1996) in Fargo. I was also a co-moderator for one of the sessions in the conference.
12. Reviewer for the following Journals: The IEEE Transactions on Multimedia, The IEEE Transactions on Information Theory, The IEEE Transactions on Reliability,

The IEEE Transactions on Computers, The IEEE Transactions on Circuits and Systems.

13. Reviewer for the following conferences:
    - The 2005 IEEE Workshop on Signal Processing Systems, Athens, Greece
    - International Conference on Parallel Processing, sponsored by IEEE and ACM. 1990 and 1993.
    - IEEE International Symposium on Circuits and Systems. 1995, 1999, 2002, 2003, 2008.
    - International Conference on High Performance Distributed Systems. 1993.
    - International Conference on Parallel and Distributed Computing Systems. 1993.
    - Midwest Symposium on Circuits and Systems. 1996.

Service to the Public

- Participated in a panel discussion on "Graduate Studies or Career Building: Which is best for you," organized by the National Society of Black Engineers, April 2010.
- Attended Conference on "Scientists Helping America," 2002. Scientists and Engineers from around the country were invited by DOD to attend this conference and help them create new ways to solve some of their technical problems and to set their research agenda.
- Licensed Yoga Teacher: Volunteer Yoga teacher, 2007-present.

Awards and Honors

1. In 2005 Intel funded 6 universities worldwide for conducting research on their IXP4xx network processor. NDSU was one of these six, the other five being, Univ. of Michigan, Portland State Univ., Univ. of California Davis, Indian Institute of Science and Tsinghua Univ.
2. Special Session on Security Systems on Silicon: Wireless and Mobile Networks: Rajendra Katti and Sudarshan Srinivasan, "Efficient Hardware implementation of a new pseudo-random bit sequence generator." Invited Paper. The IEEE International Symposium on Circuits and Systems, Taipei, Taiwan, May 2009.
3. Invited paper for the Special Session on New Generation Architectures/Implementations for Security Protocols & Cryptography Applications, Xiaoyu Ruan, Rajendra Katti, and David Hinkemeyer, "Algorithm and implementation of signed binary recoding with asymmetric digit sets for elliptic curve cryptosystems," The International Symposium on Circuits and Systems, Kos, Greece, 2006.
4. The following paper was judged one of 10 best papers in the area of hardware for cryptography. Rajendra Katti and J. Brennan, "Low Complexity Multiplication in a finite field using ring representation," The IEEE Transactions on Computers, Special Section on Cryptographic Hardware and Embedded Systems, Guest Editors, C. K. Koc and C. Paar, pp. 418-427, April 2003.
5. Intel Award for contributions toward the development of Pentium IV production test suites, Oct. 2000.

6. Invited to attend "The Scientists Helping America Conference," sponsored by DoD. The attendees were expected to think out-of-the-box and provide new ideas for research at the Department of Defence, 2003.
7. The following paper got 2nd prize in the student paper contest. This contest is held by one of the premier conferences on Bioengineering. D. M. Schneider, C. M. Ripplinger, K. Gilbertson, Rajendra Katti, and M. J. Schroeder, "Optically-based control of a Prosthetic Device," 2003 Summer Bioengineering Conference, Key Biscayne, Florida, June 25 –29, 2003.
8. Awarded the NSF Research Initiation Award, 1993.