

Kurt R. Rohloff

Curriculum Vitae

rohloff@njit.edu

New Jersey Institute of Technology

Newark NJ, 07102

RESEARCH INTERESTS

Encrypted computing, lattice encryption implementation, homomorphic encryption, cryptographic program optimization, high assurance software, secure communication protocol design, censorship circumvention technologies, system verification and certification, scalable computing, resource sharing, tactical information management.

EDUCATION

- **Ph.D. in Electrical Engineering: Systems**
The University of Michigan, Ann Arbor, MI (4/04)
 - Thesis: Computations on Distributed Discrete-Event Systems
 - Advisor: Prof. Stéphane Lafortune
 - Honorable Mention, University of Michigan Distinguished Dissertation Award (University-wide award, one nomination per department.)
 - Thesis work resulted in new approaches to the automated analysis, diagnosis and control of distributed systems.
- **M.S. of Electrical Engineering: Systems**
The University of Michigan, Ann Arbor, MI (4/01)
 - Major Area: Control
 - Minor Area: Computers: Intelligent Systems
- **B. of Electrical Engineering**
Georgia Institute of Technology (6/99)
 - GPA: 3.83/4.00
 - Graduated with Highest Honors

PROFESSIONAL POSITIONS HELD

New Jersey Institute of Technology, Newark, NJ (Sept. 2014 - present)

Associate Professor of Computer Science: Faculty at a major public research university. Research activities focusing on secure computing research, overseeing graduate students and teaching courses in cybersecurity. Staff includes professional (non-student) scientists, an associate research professor, programmers, and affiliated graduate students.

Project achievements include:

- **DARPA SafeWare:** Principal Investigator for a multi-year, multi-million dollar DARPA-funded R&D effort to develop initial prototype of encrypted program obfuscation capability. Developed the first ever implementation of cryptographic program obfuscation technique in software that operates on conjunction programs and improved runtime performance by four orders of magnitude in under a year.

Subcontracted team members and project partners include MIT, UCSD, Raytheon BBN Technologies and Vencore Labs. Led development best-of-breed open-source lattice encryption software to support cryptographic program obfuscation that is being used across our project team.

- **NSA PARAPET:** Principal Investigator for an NSA-funded project to research and develop highly scalable encrypted computing technologies to revolutionize information brokering with cloud-based data stores. Resulted in a first-ever prototype information brokering service secured with proxy re-encryption technology to protect confidentiality of shared information. Prototype was deployed in a live network and experimentally evaluated.
- **IARPA RAMPARTS:** Subcontract PI for an IARPA-funded seedling project to research and develop programming tools for computing on encrypted data. Partnered with industry performer Galois, Inc. on project. Project is resulting in a first-ever domain-specific-language to make encrypted computing easier to use and deploy.

Founding Director of NJIT Cybersecurity Research Center: Co-Founder and Director of a multi-disciplinary research center housed in the College of Computing Sciences at NJIT. Oversaw the growth of the center from \$0 in funding to over \$10M in 2 years with a current staff of 4 tenure-track faculty, a full-time externally funded research professor, staff scientists, multiple PhD students, MS students and undergraduate programmers. Oversaw the renovation of the center's facilities including dedicated office space for 20 students and a dedicated meeting center. Successes include the foster of extensive government sponsorship and industry technical partnerships. Government sponsors include DARPA, IARPA, HSARPA, NSA, NSF, ARL and US Navy SPAWAR. Industry technology partners include Raytheon BBN Technologies, Applied Communication Sciences / Vencore Labs, Invincea Labs, Galois Inc., Cybernetica AS and Lucent Government Systems.

Avometric LLC, West Orange, NJ (Aug. 2015 - present)

Founder and Chief Scientist: Founder of a boutique defense R&D consulting firm. Projects funded by subcontract for multiple Air Force Research Laboratory (AFRL) Small Business Innovation Research (SBIR) Phase 1 and Phase 2 project awards. Supporting industry partners in the design of secure enterprise software management and access control systems. Technology transition targets support Air Force Materiel Command (AFMC) and United States Strategic Command (USSTRATCOM).

Raytheon BBN Technologies, (Originally BBN Technologies) Cambridge, MA (Sept. 2005 – August 2014)

Senior Scientist: PI for multiple federally funded research and development projects related to large-scale computing, secure computing and tactical information management. Project achievements include:

- **PROCEED:** Principal Investigator for a multi-year, multi-million dollar DARPA-funded R&D effort. Project goal was to transition cutting edge theoretical design of a new encrypted computing technology into a nearly practical hardware and software implementation. Project successes include reduction in hardware and

software run-time of fully homomorphic encryption implementations by 6+ orders of magnitude. Resulted in an iPhone-based capability for encrypted full-duplex teleconferencing that is both secure and practical for real-world use and an FPGA-based co-processor for hardware-accelerated encrypted computing.

- **SCIMITAR:** Principal Investigator for an AFRL-funded project to research and develop highly scalable information management technologies and research cloud solutions for information brokering. Project resulted in a novel prototype for highly scalable and low-latency information brokering based on open-source cloud computing technologies deployed in the Amazon AWS environment.

The University of Illinois at Urbana-Champaign, Coordinated Science Laboratory (July 2004 – Aug. 2005).

Postdoctoral Research Associate: Supervised by Prof. Tamer Başar, member of the US National Academy of Engineering and European Academy of Sciences. Researched and developed innovative stochastic modeling techniques for the automated detection of computer worm epidemics based on real-time data analysis of information network measurements during Internet worm propagation.

CWI, Centrum Wiskunde & Informatica (Center for Mathematics and Computation), Amsterdam, the Netherlands (Summer 2003).

Visiting Researcher: Supervised by Prof. Dr. Jan H. van Schuppen. Researched and developed risk models and algorithms to solve real-time optimal sensor selection problems for supervisory control in risk-averse distributed systems.

MIT Lincoln Laboratory, Lexington, MA (Summers of 1999, 2000)

Visiting Researcher: Developed control and simulation models of ICBM flights for the THAAD missile defense system program. Researched and developed machine-learning pattern recognition techniques to for target identification and tracking in the NMD missile defense system program.

MAJOR OPEN SOFTWARE PROJECTS

- **PALISADE**

Chief architect of PALISADE, a best-of-breed open-source library for lattice-based cryptography. This library provides implementation of multiple post-quantum Public Key, Digital Signature Systems, Proxy Re-Encryption, Homomorphic Encryption and Cryptographic Program Obfuscation cryptographic protocols. The library is a rapid-prototyping tool that provides general and adoptable lattice-based cryptographic primitives including ring arithmetic, number theoretic transforms and lattice-based trapdoors on top of an extensible custom library of modular mathematics primitives.

The PALISADE library is currently in beta release for our funded technology partners on the 2-clause BSD license. PALISADE is under active development with sponsorship from DARPA, NSA and IARPA, and is contributing to project success on the DARPA SafeWare and IARPA RAMPPTS projects. Current developers, contributors and evaluators of the PALISADE library include NJIT, MIT and UCSD from academia and Raytheon BBN, ACS/Vencore Labs, LGS Innovations, Galois Inc. and Invincea Labs from industry.

- **SHARD**

Chief architect and originator of a proof-of-concept cloud-based, highly scalable graph data storage and information retrieval technology. SHARD is built on top of the Cloudera Hadoop distribution to support highly scalable querying over Semantic Web graph data. The SHARD triple-store was evaluated to respond an order of magnitude faster than best-of-breed commercial graph-store technologies. Although not under active development, the SHARD triple-store has been downloaded and used to benchmark subsequent cloud computing software solutions by industry and academic colleagues. SHARD was publicly released on a 2-clause BSD license in 2010 and has not been under active public development since then.

GRANTS AND CONTRACT AWARDS

- DARPA I2O, SafeWare, PALISADE. \$3.4M, Principal Investigator. ARL contract W911NF-15-C-0226. Subcontracts to Raytheon BBN Technologies, MIT and UCSD. Period of Performance: 2015-2019.
- DARPA I2O SafeWare OPERA, Subcontracted to Applied Communication Sciences / Vencore Labs. Subcontract PI. NJIT award: \$674K. ARL contract -15-C-0233. Period of Performance: 2015-2019.
- IARPA Safe and Secure RAMPARTS Seedling Subcontracted to Galois, Inc. Subcontract PI. NJIT Award: \$393K. Period of Performance: 2016-2017.
- PARAPET, NSA. Principal Investigator. NJIT Award: \$298K. NSA grant H98230-15-1-0274. Period of Performance: 2015-2016.
- DARPA TCTO/I2O. PROgramming Computation on EncryptEd Data (PROCEED), SIPHER Subcontracted to Raytheon BBN Technologies. Subcontract PI. NJIT Award: \$173K. AFRL contract FA8750-11-C-009. Period of Performance: 2014-2015.
- DARPA TCTO/I2O. PROgramming Computation on EncryptEd Data (PROCEED), SIPHER Principal Investigator. Raytheon BBN Technologies Total Award: \$3M AFRL contract FA8750-11-C-009 Subcontractors: Georgia Institute of Technology. Period of Performance: 2011-2015.
- AFRL Information Directorate, Scalable Information Management Technology And Research (SCIMITAR). Raytheon BBN Technologies Award: \$700K (approx.). AFRL contract award FA8750-12-C-0083. Period of Performance: 2012-2013.
- META, DARPA STO. Contract award HR0011-10-C-0108, \$2M (aprox.) (Tech Lead). Period of Performance: 2009-2011.
- International Crisis Early Warning System (ICEWS), DAPRA IPTO. AFRL/HECS contract FA8650-07-C-774, \$6M (approx.). (Tech Lead) Period of Performance: 2007-2009.

Additional proprietary contracts awards were made but cannot be listed without prior approval from the associated contracting agencies. Except for the awards which cannot be listed without prior approval, contract awards are listed only if K. Rohloff had a substantial role in both business development and contract execution. Additional awards were made which fit only one but not both of these criteria.

TEACHING

- **Network Management and Security, NJIT CS 696.**
 - 3 credit-hour lecture course.
 - Course size: 36 students
 - Redesigned this graduate-level course on network management and security to better align with industry-focused educational needs. Course now focuses on case-based studies of network management challenges and pressing security needs to better prepare students for later success in industry. Course focuses on analysis of adversarial behavior and protecting networks from adversarial behavior.
 - Recorded lectures and prepared course material for an online distance version of the course.
 - Course offerings with overall student rating of educational value:
 - In-person offering:
 - Fall 2014. Rating: 3.58/4.00
 - Fall 2015. Rating: 3.27/4.00
 - Distance offering:
 - Spring 2015. Rating: 3.13/4.00
 - Spring 2016. Rating: 3.00/4.00
- **Fundamentals of Network Security, NJIT CS 357.**
 - 3 credit-hour lecture course.
 - Course size: 36 students
 - Redesigned this undergraduate-level course on network management and security to better align with industry-focused educational needs. Course now focuses on case-based studies of network security challenges and high-level design challenges faced by network management and design staff in real-world settings.
 - Course offerings:
 - In-person offering: Fall 2016. (Course not rated by students yet.)

PUBLICATIONS

Journals

- J1. Yuriy Polyakov, Kurt Rohloff, Gyana Sahu and Vinod Vaikuntanathan. "Fast Proxy Re-Encryption for Publish/Subscribe Systems", Under Review in ACM Transactions on Privacy and Security (ACM TOPS).
- J2. Cristian Borcea, Arnab "Bobby" Deb Gupta, Yuriy Polyakov, Kurt Rohloff, Gerard Ryan, "PICADOR: End-to-End Encrypted Publish-Subscribe Information Distribution with Proxy Re-Encryption" Accepted to Future Generation Computing Systems (FGCS)
- J3. David Bruce Cousins, Kurt Rohloff and Daniel Sumorok. "Accelerating Secure Computing with a Dedicated FPGA-based Homomorphic Encryption Co-Processor." Accepted to IEEE Transactions on Emerging Topics for Computing (IEEE TETC).
- J4. Kurt Rohloff, David Bruce Cousins and Daniel Sumorok. "Scalable, Practical VoIP Teleconferencing with End-to-End Homomorphic Encryption." Accepted to IEEE Transactions on Information Forensics and Security (IEEE TIFS).
- J5. Dave W. Archer, Kurt Rohloff "Computing with Data Privacy: Steps Toward Realization." in IEEE Security & Privacy (IEEE S&P), vol. 13, no. 1, pp. 22-29, Jan.-Feb. 2015.
- J6. Kurt Rohloff and Tamer Başar. "Deterministic and Stochastic Models for the Detection of Random Constant Scanning Worms." ACM Transactions on Modeling and Computer Science (ACM TOMACS) Special Issue on Simulation, Modeling and Security. Volume 18, Number 2, April 2008.
- J7. Kurt Rohloff, Samir Khuller and Guy Kortsarz. Approximating Optimal Sensor Selections and Connections to Colored st-cut Problems, Discrete-Event Dynamic Systems: Theory and Applications (DEDS). Volume 16, Number 1, Jan. 2006.
- J8. Kurt Rohloff and Stéphane Lafortune. The Verification and Control of Interacting Similar Discrete-Event Systems, SIAM Journal on Control and Optimization (SICON). Volume 45, Number 2, Jan. 2006.
- J9. Kurt Rohloff, Joseph Loyall, Richard Schantz. Quality Measures for Embedded Systems and Their Application to Control and Certification, ACM SIGBED Review, Special Issues on Workshop on Innovative Techniques for Certification of Embedded Systems. Volume 3, Number 4, October 2006.
- J10. Kurt Rohloff, Stéphane Lafortune. PSPACE-completeness of Automata Intersection with Applications to Supervisory Control of Discrete-Event Systems. Discrete-Event Dynamic Systems: Theory and Applications (DEDS), 15:2 June, 2005.
- J11. Kurt Rohloff, Tae-Sic Yoo, Stéphane Lafortune. Deciding Coobservability is PSPACE-complete. IEEE Transactions of Automatic Control (IEEE TAC), 48:11. November, 2003

- J12. Kurt Rohloff, Stéphane Lafortune. On the Synthesis of Safe Control Policies in Decentralized Control of Discrete Event Systems. IEEE Transactions of Automatic Control (TAC). 48:6, pg.1064-1068. June, 2003

Conferences and Workshops

- C1. Giovanni Di Crescenzo, Lisa Bahler, Brian A. Coan, Yuriy Polyakov, Kurt Rohloff, David Bruce Cousins. "Practical implementations of program obfuscators for point functions." HPCS 2016: 460-467
- C2. Arnab Deb Gupta, Yuriy Polyakov, Kurt Rohloff and Gerard Ryan, "Securely Sharing Encrypted Medical Information," 2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Washington, DC, June 28, 2016, pp. 330-331.
- C3. Arnab Deb Gupta, Yuriy Polyakov, Kurt Rohloff "Secure Medical Information Access Delegation." 10th International Symposium on Medical Information and Communication Technology (ISMICT 2016). Mar. 21-23, 2016.
- C4. Kurt Rohloff "Privacy-Preserving Data Exfiltration Monitoring Using Homomorphic Encryption." The 2nd IEEE International Conference on Cyber Security and Cloud Computing. Nov. 3-5, 2015.
- C5. Kurt Rohloff, Yuriy Polyakov "An End-to-End Security Architecture to Collect, Process and Share Wearable Medical Device Data." 17th International Conference on E-health Networking, Application & Services (HealthCom). Oct. 14-17 2015.
- C6. David Bruce Cousins, John Golusky, Kurt Rohloff, Daniel Sumorok "An FPGA Co-Processor Implementation of Homomorphic Encryption." IEEE High Performance Extreme Computing Conference (HPEC). Jan. 6 2014.
- C7. Kurt Rohloff, David Bruce Cousins. "A Scalable Implementation of Fully Homomorphic Encryption Built on NTRU." 2nd Workshop on Applied Homomorphic Cryptography and Encrypted Computing (WAHC). Mar. 7, 2014.
- C8. Kurt Rohloff, Jeffrey Cleveland, Kyle Usbeck "Scalable Streaming Graph Data Processing: A Position Paper on Design Goals and a Possible Approach." Big Data Analytics: Challenges and Opportunities (BDAC-13). In Cooperation with ACM/IEEE SC13. Nov. 17, 2013.
- C9. Kurt Rohloff, Jeffrey Cleveland, Joseph Loyall, Timothy Blocher "SCIMITAR: Scalable Stream-Processing for Sensor Information Brokering." Military Communications Conference (MILCOM), Nov. 18-20, 2013.
- C10. Kurt Rohloff, Jeffrey Cleveland, Kyle Usbeck "The AQUEDUCT Streaming Linked Data Processing Capability in a Scalable Cloud Computing Framework." Semantic Technology & Business Conference, Jun. 2-5, 2013.

- C11. Kurt Rohloff, Kyle Usbeck, Joe Loyall “GAMETE: General Adaptable Metric Execution Tool and Environment.” 3rd International Workshop on Model-driven Approaches for Simulation Engineering (Mod4Sim), Apr. 7-10, 2013.
- C12. Kurt Rohloff “Bounded Sensor Failure Tolerant Supervisory Control.” 11th International Workshop on Discrete-Event Systems (WODES), Oct. 3-5, 2012.
- C13. David Bruce Cousins, Kurt Rohloff, Chris Peikert, Rick Schantz. “An update on Scalable Implementation of Primitives for Homomorphic EncRyption - FPGA implementation using Simulink.” Sixteenth Annual Workshop on High Performance Embedded Computing (HPEC), Sept. 10, 2012.
- C14. Ipek Kaynar Rohloff, Kurt Rohloff. “Modeling Spatial Activity Distributions in Complex Urban Conditions: The Markov Chain Model for Weighting Spaces with Attractors.” 100th ACSA Annual Meeting; Massachusetts Institute of Technology, Cambridge, March 1-4, 2012.
- C15. David Bruce Cousins, Kurt Rohloff, Chris Peikert, Rick Schantz. “SIPHER: Scalable Implementation of Primitives for Homomorphic EncRyption - FPGA implementation using Simulink.” Fifteenth Annual Workshop on High Performance Embedded Computing (HPEC), Sept. 21, 2011.
- C16. Kurt Rohloff, Joseph Loyall. “An Ontology for Resource Sharing.” Fifth IEEE International Conference on Semantic Computing (ICSC) Workshop on Ontologies for Systems Integration and Standards, Sept. 18, 2011.
- C17. Kurt Rohloff, Richard Schantz. “Clause-Iteration with Map-Reduce to Scalably Query Data Graphs in the SHARD Graph-Store.” DIDC 2011: Fourth International Workshop on Data Intensive Distributed Computing. June 8, 2011
- C18. Joseph Loyall, Kurt Rohloff, Partha Pal, Michael Atighetchi. “A Survey of Security Concepts for Common Operating Environments.” WORNUS 2011: 2nd IEEE International Workshop on Object/component/service-oriented Real-time Networked Ultra-dependable Systems. March 28-31 2011.
- C19. Kurt Rohloff, Rick Schantz. “High-Performance, Massively Scalable Distributed Systems using the MapReduce Software Framework: The SHARD Triple-Store.” International Workshop on Programming Support Innovations for Emerging Distributed Applications (PSI EtA), 2010.
- C20. Partha Pal, Kurt Rohloff, Michael Atighetchi, and Rick Schantz. “Managed Mission Assurance: Concept, Methodology and Runtime Support.” Workshop on Mission Assurance: Tools, Techniques, and Methodologies at the 2nd IEEE International Conference on Privacy, Security, Risk, and Trust. August 20-22 2010, Minneapolis, Minnesota, USA.
- C21. Partha Pal, Rick Schantz, Michael Atighetchi, Kurt Rohloff, Nathan Dautenhahn and William Sanders. “Fighting Through Cyber Attacks: An Informed Perspective Toward

the Future.” Workshop on Survivability in Cyberspace, Part of CPS Week 2010, April 2010.

- C22. Kurt Rohloff, Partha Pal, Michael Atighetchi, Richard Schantz, Kishor Trivedi and Christos Cassandras. “Approaches to Modeling and Simulation for Dynamic, Distributed Cyber-Physical Systems.” Workshop on Grand Challenges in Modeling, Simulation, and Analysis for Homeland Security (MSAHS-2010), March 2010.
- C23. Kurt Rohloff, Robert Battle, Jim Chatigny, Rick Schantz and Victor Asal. “A Trend Pattern Approach to Forecasting Socio-Political Violence.” Third International Conference on Computational Cultural Dynamics, Dec. 2009.
- C24. Kurt Rohloff. “Automated Discovery and Modeling Of Sequential Patterns Preceding Events of Interest.” ModSim World, Oct. 2009.
- C25. Kurt Rohloff and Paul Rubel. “Discovering Automated Sequential Patterns the Precede Outbreaks of Socio-Political Violence.” HSCB Focus 2010, August, 2009.
- C26. Partha Pal, Rick Schantz, Kurt Rohloff and Joseph Loyall. Cyber-physical Systems Security - Challenges and Research Ideas. Workshop on Future Directions in Cyber-physical Systems Security, July 2009.
- C27. Kurt Rohloff and Wayne Thornton. “A Knowledge Environment for Social Science Exploration.” Human Behavior-Computational Intelligence Modeling Conference, June 2009.
- C28. Rick Schantz, Jake Beal, Joe Loyall, Partha Pal, Kurt Rohloff and Azer Bestavros. “Research Challenges in Information Systems for the Next Generation Electric Grid.” National Workshop on New Research Directions for Future Cyber-Physical Energy Systems, June 2009.
- C29. Kurt Rohloff and Victor Asal. “Computational Methods to Discover Sets of Patterns of Behaviors that Precede Political Events of Interest.” AAAI Spring Symposium on Technosocial Predictive Analytics, March 2009.
- C30. Joseph Loyall, Partha Pal, Kurt Rohloff and Matthew Gillen. “Issues in Context-Aware and Adaptive Middleware for Wireless, Mobile Networked Systems.” Workshop on Research Directions in Situational-aware Self-managed Proactive Computing in Wireless Adhoc Networks, March 2009
- C31. Robert Battle, Douglas Reid, Kurt Rohloff. “CWEST: Disruptive Integration of Computation Technology for Data Analysis and Visualization.” Visualizing the Past: Tools and Techniques for Understanding Historical Processes, February 2009.
- C32. Kurt Rohloff and Victor Asal. “The Identification of Sequential Patterns Preceding the Occurrence of Political Events of Interest.” Second International Conference on Computational Cultural Dynamics, September 2008.

- C33. Kurt Rohloff. "Directions for Cost-Effective Certification of High-Assurance Cyber Physical Systems." Fourth Annual Carnegie Mellon Conference on the Electricity Industry, March 2008.
- C34. Kurt Rohloff, Mike Dean, Ian Emmons, Dorene Ryder, John Sumner "An Evaluation of Triple-Store Technologies for Large Data Stores" 3rd International Workshop On Scalable Semantic Web Knowledge Base Systems (SSWS '07), Vilamoura, Portugal, Nov 27, 2007
- C35. Matthew Gillen, Kurt Rohloff, Prakash Manghwani, and Richard Schantz. "Scalable, Adaptive, Time-Bounded Node Failure Detection " 10th IEEE High Assurance Systems Engineering (HASE) Symposium, Dallas, Texas, November 14 - 16, 2007
- C36. Kurt Rohloff, Joseph Loyall, Partha Pal, and Richard Schantz. "High-Assurance Distributed, Adaptive Software for Dynamic Systems" 10th IEEE High Assurance Systems Engineering (HASE) Symposium Dallas, Texas November 14 - 16, 2007.
- C37. Kurt Rohloff, Richard Schantz and Yarom Gabay. "High-Level Dynamic Resource Management for Distributed, Real-Time Embedded Systems." 5th Symposium on Design, Analysis and Simulation of Distributed Systems (DASD), San Diego, CA, 2007.
- C38. Kurt Rohloff, Yarom Gabay, Jianming Ye and Richard Schantz. "Scalable, Distributed, Dynamic Resource Management for the ARMS Distributed Real-Time Embedded System." International Workshop on Parallel and Distributed Real-Time Systems (WPDRTS) Long Beach, CA, 2007.
- C39. Kurt Rohloff, Richard Schantz, Partha Pal and Joseph Loyall. "Software Certification for Distributed, Adaptable Medical Systems: Position Paper on Challenges and Paths Forward." Joint Workshop On High Confidence Medical Devices, Software, and Systems (HCMDSS) and Medical Device Plug-and-Play (MD PnP) Interoperability, June 25-27, 2007, Boston, MA.
- C40. Kurt Rohloff, Richard Schantz and Joseph Loyall. Dynamic, High Confidence Certifiable Embedded Software: Position Paper, 2006 National Meeting, Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, November 8 & 9, 2006, Pittsburgh, Pennsylvania.
- C41. Kurt Rohloff, Jianming Ye, Joseph Loyall, Richard Schantz. A Hierarchical Control System for Dynamic Resource Management, 2006 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2006), Work in Progress Symposium. April 7, 2006, San Jose, CA.
- C42. Kurt Rohloff, Joseph Loyall, Richard Schantz. Quality Measures for Embedded Systems and Their Application to Control and Certification, 2006 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS 2006), Workshop on Innovative Techniques for Certification of Embedded Systems. April 4, 2006, San Jose, CA.

- C43. Kurt Rohloff "Sensor Failure Tolerant Supervisory Control" 44th IEEE Conference on Decision and Control, 2005 and 2005 European Control Conference. CDC-ECC '05. Dec. 12-15, 2005.
- C44. Kurt Rohloff and Tamer Başar. The detection of RCS worm epidemics. In Proceedings of the 2005 ACM Workshop on Rapid Malcode (WORM), November 11, 2005.
- C45. Kurt Rohloff and Tamer Başar. "Stochastic behavior of random constant scanning worms," 14th International Conference on Computer Communications and Networks (ICCCN) Oct. 17-19, 2005.
- C46. Kurt Rohloff, The Diagnosis of Failures via the Combination of Distributed Observations, Mediterranean Conference on Decision and Control, 2005.
- C47. Kurt Rohloff, Jan H. van Schuppen. Approximating Minimal Communicated Event Sets for Decentralized Supervisory Control, IFAC World Congress, 2005.
- C48. Kurt Rohloff, Tansu Alpcan, Tamer Başar. A Discrete-Event Systems Model for Congestion Control, IFAC World Congress, 2005.
- C49. Kurt Rohloff. Information Acquisition, Approximation Algorithms and Supervisory Control. Workshop on Control of Hybrid and Discrete Event Systems (CHyDES'05), a satellite event of the 26th International Conference On Application and Theory of Petri Nets and Other Models of Concurrency (ATPN 2005). Miami Florida, June 21, 2005.
- C50. Kurt Rohloff, Samir Khuller, Guy Kortsatz. Approximating Optimal Sensor Selections for Supervisory Control, Workshop on Discrete-Event Systems, 2004. (Invited to submit a journal version of this paper to a special edition of the journal Discrete Event Dynamic Systems.)
- C51. Kurt Rohloff, Stéphane Lafortune. Symmetry Reductions for a Class of Modular Discrete-Event Systems, Conf. on Decision and Control, 2004.
- C52. Kurt Rohloff, Stéphane Lafortune. The Control and Verification of Similar Agents Operating in a Broadcast Network, Conf. on Decision and Control, 2003.
- C53. Kurt Rohloff, Stéphane Lafortune. Supervisor Existence for Modular Discrete-Event Systems, Proc. of the 2nd IFAC Conf. on Control Systems Design, 2003.
- C54. Kurt Rohloff, Stéphane Lafortune. Recent Results on Computational Issues in Supervisory Control, Proc. of the ATPN-Workshop Discrete Event Systems Control, 2003.
- C55. Kurt Rohloff, Stéphane Lafortune. On the Computational Complexity of the Verification of Modular Discrete-Event Systems, Conf. on Decision and Control, 2002.

Book Chapters

- B1. Stéphane Lafortune, Kurt Rohloff, Tae-Sic Yoo. Recent Advances on the Control of Partially-Observed Discrete-Event Systems. In *Synthesis and Control of Discrete Event Systems*. Benoît Caillaud, Philippe Darondeau, Luciano Lavagno and Xiaolan Xie, eds.,

Edited Volumes

- E1. Jeremy Clark, Sarah Meiklejohn, Peter Y. A. Ryan, Dan S. Wallach, Michael Brenner, Kurt Rohloff: *Financial Cryptography and Data Security - FC 2016 International Workshops, BITCOIN, VOTING, and WAHC*, Christ Church, Barbados, February 26, 2016, Revised Selected Papers. *Lecture Notes in Computer Science 9604*, Springer 2016, ISBN 978-3-662-53356-7
- E2. Michael Brenner, Nicolas Christin, Benjamin Johnson, Kurt Rohloff: *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable*, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers. *Lecture Notes in Computer Science 8976*, Springer 2015, ISBN 978-3-662-48050-2

Technical Reports

- T1. David Cousins, Kurt Rohloff, Christopher Peikert, Daniel Sumorok. “SIPHER: Scalable Implementation of Primitives for Homomorphic Encryption”. DTIC Accession Number ADA624640
- T2. Richard E. Schantz, Joseph P. Loyall, Kurt Rohloff, Jianming Ye, Prakash Manghwani, Yarom Gabay, Yarom, Priya Narasimhan, Aaron Paulos, Aniruddha Gokhale, Jaiganesh Balasubramanian. *Adaptive Multilevel Middleware for Object Systems*. DTIC Accession Number ADA465928
- T3. Kurt Rohloff, Stéphane Lafortune. *Advances in State Estimation and Controller Synthesis for General Decentralized Control of Discrete Event Systems*, University of Michigan EECS Technical Report CGR-01-11
- T4. Kurt Rohloff, Stéphane Lafortune. *Deciding Coobservability is PSPACE-complete*, University of Michigan EECS Technical Report CGR-03-06
- T5. Kurt Rohloff, Stéphane Lafortune. *Space Efficient Methods for Testing Reachability with Applications to Coobservability and Decentralized Control*, University of Michigan EECS Technical Report CGR-03-08
- T6. Kurt Rohloff, Stéphane Lafortune. *Symmetry Reductions for a Class of Distributed Discrete-Event Systems*, University of Michigan EECS Technical Report CGR-04-02
- T7. Kurt Rohloff, Jan H. van Schuppen. *Approximating the Minimal-Cost Sensor-Selection for Discrete-Event Systems*. CWI Report MAS-R0404, CWI, Amsterdam, The Netherlands, December 2004.

Professional Seminars

- S1. Kurt Rohloff. “Everything you Wanted to Know about DARPA but were Afraid to Ask.” New Jersey Institute of Technology Computer Science Seminar, September 19, 2016.

- S2. Kurt Rohloff. "Implementing Homomorphic Encryption to Enable Practical and Secure Computing" University of Tartu Computer Science Research Seminar, March 15, 2016
- S3. Kurt Rohloff. "Applying Homomorphic Encryption for Practical Genomic Privacy" Dagstuhl Seminar 15431, Dagstuhl, Germany, October 20, 2015.
- S4. Kurt Rohloff. "Privacy-Preserving Publish-Subscribe using End-to-End Encryption" Workshop on Surveillance & Technology held with the Privacy Enhancing Technologies Symposium (PETS). Philadelphia PA. June 29th, 2015
- S5. Kurt Rohloff. "Towards Practical Implementations of Fully Homomorphic Encryption" City University of New York, Algebra and Cryptography Seminar, September 12, 2014
- S6. Kurt Rohloff. "Enabling Practical Secure Computing through Fully Homomorphic Encryption", New Jersey Institute of Technology Computer Science Seminar, January 27, 2014.
- S7. Kurt Rohloff. "Enabling Secure Computing through Fully Homomorphic Encryption", Mount Holyoke College Math and Stat Seminar, November 13, 2013.
- S8. Kurt Rohloff. "Enabling Practical Secure Computing through Fully Homomorphic Encryption", Worcester Polytechnic Institute, November 6, 2013.
- S9. Kurt Rohloff. "Enabling Secure Computing through Fully Homomorphic Encryption" University of Massachusetts Amherst Computer Science Research Seminar, March 26, 2013
- S10. Kurt Rohloff. "Modeling and Detecting the Propagation of Internet Worm Epidemics". Georgia Tech School of Industrial and Systems Engineering Seminar. November 7, 2012.
- S11. Kurt Rohloff. "Cloud computing for Scalability: The SHARD Triple-Store." Cambridge SemWeb MeetUp, January 9, 2011.
- S12. Kurt Rohloff. "Cloud computing for Scalability: The SHARD Triple-Store." SemWeb MeetUp Webcast, January 9, 2011.
- S13. Kurt Rohloff. "SHARD: Cloud-Computing for a Scalable Semantic Web." Tufts University Computer Science Colloquium. September 16, 2010.
- S14. Kurt Rohloff. "SHARD: Storing and Querying Large-Scale SemWeb Data." HadoopWorld, 2010.
- S15. Kurt Rohloff. "Cloud- and Cluster-Computing Technologies for the Semantic Web." Semantic Technology Conference, 2010.

PATENTS

- P1. Kurt Rohloff "System and method to merge encrypted signals in distributed communication system." U.S. Patent No. 9,461,974. October 4, 2016.
- P2. Kurt Rohloff and David Bruce Cousins. "System and Method for Mixing VoIP Streaming Data for Encrypted Processing" U.S. Patent No. 9,369,273. June 14, 2016
- P3. Kurt Rohloff. "System and method for operating on streaming encrypted data." U.S. Patent No. 9,338,144. May 10 2016.
- P4. Kurt Rohloff. "System and method for merging encryption data using circular encryption key switching." U.S. Patent No. 9,325,671. April 26, 2016.
- P5. Kurt Rohloff "System and method to merge encrypted signals in distributed communication system." U.S. Patent No. 9,313,181. April 12, 2016.

PATENT APPLICATIONS

- A1. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MERGING ENCRYPTION DATA WITHOUT SHARING A PRIVATE KEY." United States Patent Application 20150304287. Filed 2014.
- A2. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD TO MERGE ENCRYPTED SIGNALS IN DISTRIBUTED COMMUNICATION SYSTEM." United States Patent Application 20150249650. Filed 2014.
- A3. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD TO MERGE ENCRYPTED SIGNALS IN DISTRIBUTED COMMUNICATION SYSTEM." United States Patent Application 20150249649. Filed 2014.
- A4. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MIXING VOIP STREAMING DATA FOR ENCRYPTED PROCESSING." United States Patent Application 20150244516. Filed 2014.
- A5. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MIXING VOIP STREAMING DATA FOR ENCRYPTED PROCESSING." United States Patent Application 20150237020. Filed 2014.
- A6. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MERGING ENCRYPTION DATA USING CIRCULAR ENCRYPTION KEY SWITCHING." United States Patent Application 20150237019. Filed 2014.
- A7. Kurt Rohloff, David Bruce Cousins and Richard Schantz. "METHOD FOR SECURE SYMBOL COMPARISON." United States Patent Application 20140233728. Filed 2013.

A8. Kurt Rohloff, David Bruce Cousins and Richard Schantz. "METHOD FOR SECURE SUBSTRING SEARCH." United States Patent Application 20140233727. Filed 2013.

ACADEMIC AWARDS AND HONORS

- NJIT College of Computing Sciences Research Award, 2016
- BBN Business Development Awards, every year 2008-2014.
- BBN Publication Awards, 2006, 2008.
- Honorable Mention for the University of Michigan Distinguished Dissertation Award, 2004 (University-wide award, one nomination per academic department.)
- GAANN (Graduate Assistance in Areas of National Need) Fellowship, 2001.
- Graduated with Highest Honors, Georgia Tech, Spring 1999.
- Georgia Tech ECE Sophomore of the Year, 1997.
- Dean's List or Faculty Honors every academic session at Georgia Tech 1995-1999.

STUDENT MENTORING

Doctoral Students

- Gyana Sahu, NJIT PhD, Expected Spring 2019.
- Hadi Sajjadpour, NJIT PhD, Expected Spring 2019.
- Gerard Ryan, NJIT PhD, Expected Spring 2019.
- Nishanth Pasham, NJIT PhD, Expected Spring 2019.

Masters Thesis Students

- Arnab Deb Gupta, NJIT MS Thesis 2016. "Secure Asynchronous Content Distribution For Distributed Information Systems."
- Mayur Agarkar, NJIT MS Thesis, 2015. "Advanced Encryption Standard Hybrid Key Chaining" Won NJIT Graduate Student Poster Showcase Award.

Masters Project Students

- Danny O'Boyle, NJIT MS Project, 2016. "Design of a Public Key Repository for Lattice Encryption Systems"
- Cassie Lebauer, NJIT MS Project, 2016. "The TALUS Homomorphic Encryption Circuit Simulator"
- Suchanda Mukherjee, NJIT MS Project, 2015 "Unit Testing in a C++ Lattice Encryption Library"

Undergraduate Student Project Mentorship

- Kamil Doruk Gur, Sabanci University, Summer 2016 and Senior project 2017. "Lattice-Based Digital Signature Systems"
- Luke Greenleaf and Omar Muhammed, NJIT, Winter 2015 "Design of a Secure NACL Communication Framework"
- Liye Fu, Mount Holyoke College, "Optimized FHE Circuit Design." Summer 2013
- Pam Bilo, Indiana University, "Fully Homomorphic Encryption Implementation." Summer 2012
- Yarom Gabay, Boston University, "Stochastic Computation Resource Allocation." Summer 2007

Non-Supervising Graduate Student Thesis Committee Memberships

- Nafi Diallo NJIT PhD Thesis Committee Member, 2016, "Termination, Correctness and Relative Correctness."
- Ruchir Arya NJIT MS Thesis Committee Member, 2016, "Towards Trustworthy Version Control System: Enhancing the Security of Subversion."
- Riivo Talise, University of Tartu, PhD. Thesis Opponent, 2016, "Applying Secure Multiparty Computation in Practice."

PROFESSIONAL AFFILIATIONS AND SERVICE

Membership:

- IEEE (1997-present)
- AAAI (2009-2010)

NJIT Service

- NJIT Faculty Research Advisory Board, 2014-2016
- NJIT CCS Search Committee for SRO Project Manager, 2015
- NJIT CS Faculty Search Committee, 2014-2015
- NJIT CS Research Committee, 2015-2016

Professional Service:

- Organizer of BBN Distributed Systems Seminar Series (2007-2014)
- Member of International Federation of Automatic Control (IFAC) Technical Committee on Discrete Event and Hybrid Systems (2005-present)
- Member of IEEE IES Technical Committee on Factory Automation (2014-2015)
- Reviewer for multiple international conferences and journals.

Conference Service:

- Co-Chair:
 - Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC), 2015, 2016, 2017
 - Innovative CyberSecurity and Privacy for Internet of Things: Strategies, Technologies, and Implementations (WICSPIT) 2017
 - Efficient and Scalable Cybersecurity Using Algorithms Protected by Electricity (ESCAPE), 2015
- Track Chair or Co-Chair:
 - IFAC Symposium, 2005
 - Conference on Decision and Control (CDC) 2005
 - Conference on Automation Science and Engineering (CASE), 2009
- Research-Industry Chair:
 - International Conference on Advanced Engineering Computing and Applications in Sciences (ADVCOMP), 2009
- Program Committee Membership:
 - International Conference on Computing, Networking and Communications (ICNC) 2017
 - International Conference on Computer Communications and Networks (ICCCN) 2007-2008, 2016
 - Workshop on Discrete-Event Systems (WODES) 2006-2008, 2016
 - IEEE Mobile Cloud, 2016
 - Second International Workshop on Mobile Cloud Computing systems, Management, and Security (MCSMS) 2016
 - Workshop on Applied Homomorphic Computing 2013-2015
 - IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), 2015
 - American Control Conference (ACC) 2008, 2013, 2014

- International Conference on Industrial Automation, Information and Communications Technology (IAICT) 2014
- Extended Semantic Web Conference (ESWC) 2013
- Engineering Technologies & Factory Automation (ETFA) 2013
- Conference on Automation Science and Engineering (CASE) 2008-2009

MEDIA EXPOSURE

- **TechNews** “新的一年，手機可能曝露在不安全中”，Jan. 5, 2016
- **CIO** “How to Overcome Roadblocks Facing the Security of Embedded Medical Devices”, June 30, 2015
- **The Christian Science Monitor** “Digital Divide Widens as the Web Adopts Stronger Encryption Standards”, Dec. 30, 2015
- **ComputerScienceMajor.org** “Director of Cybersecurity Research – Kurt Rohloff”, Nov 20, 2015
- **CIO** “How Fully Homomorphic Encryption Can Prevent Infiltration of Secure Networks”, Nov. 10 2015
- **CivSource Online** “Cybersecurity Month: Private Sector Struggles with Government Stance on Encryption”, Oct. 29 2015
- **In Homeland Security** “CIA Director: Email Hack a Reminder of Increasing Cyber Vulnerability”, Oct. 29, 2015
- **Homeland Security Today** “CIA Director: Email Hack a Reminder of Increasing Cyber Vulnerability”, Oct. 28, 2015
- **SecurityLab.ru** “DARPA создаст способы борьбы с реверс-инжинирингом программ”, Sept 17, 2015
- **Security Affairs** “DARPA even more interested in software Obfuscation Solutions” Sept. 16, 2015
- **Foreign Policy** “Situation Report”, Sept. 15, 2015
- **Signal**, “DARPA Dabbles with Software Obfuscation Solutions”, Sept 14 2015
- **MeriTalk** “DARPA Researchers Begin Hunt for Unhackable Code”, Sept 8, 2015
- **Cirius Blog** “The Value of Secure Messaging: Lessons from the OPM Data Breach” July 23, 2015
- **Voice of America** “Encryption Debate Comes Out of the Shadows”, July 13, 2015
- **Federal Times** “OPM Breach a Failure on Encryption, Detection”, June 19, 2015
- **Senate Republican Conference** “Cybersecurity: ‘It’s Impossible To Overstate This Threat’” June 11, 2015
- **USA Today** “Senate Bill Would Help Thwart Hackers, Expert Says”, June 9, 2015
- **Avant Research Group Blog** “Senate Bill Would Help Thwart Hackers, Expert Says” June 10, 2015
- **Window IT Pro** “IT Innovators: Creating an Open Source Solution to Help IT Professionals Secure their Data in the Cloud”, May 4, 2015
- **Dr. Dobb's**. “Movement on the Big Data Front”, Apr. 8, 2010.
- **Cloudera Blog**, “How Raytheon BBN Technologies Researchers are Using Hadoop to Build a Scalable, Distributed Triple Store”, Mar. 22, 2010
- **Target Health Global** "A Plan to Catch the Conficker Worm" Apr. 1, 2009
- **MIT Technology Review**, “A Plan to Catch the Conficker Worm”, Mar. 30, 2009
- **КОМПЬЮЛЕНТА** “Остановить паразита” June 26, 2008
- **MIT Technology Review**, “Containing Internet Worms”, Jun. 12, 2008