Kurt R. Rohloff

Curriculum Vitae

Start-up:	Academic:
Duality Technologies	New Jersey Institute of Technology
Newark, NJ 07103	Newark NJ, 07102
krohloff@duality.cloud	rohloff@njit.edu

BRIEF RESEARCH INTEREST STATEMENT

My research interests are the use of cryptography, algorithm and data structure design, software engineering, systems engineering, cybersecurity design approaches and hardware acceleration to enable encrypted computing, particularly supported by lattice-based cryptography. My main research products are an advanced open-source lattice cryptography library called PALISADE currently in use in the US defense industry and an encrypted data science start-up I co-founded.

I have structured my research career to intermittently focus on traditional DARPA-funded basic academic research which I then mature and transition into operational use. I have repeated this cycle several times in the military domain and am currently developing a start-up, Duality Technologies, based on my collaborators' and my research. I plan on continuing this cycle between research and application over the extent of my career, while based at a major academic research university.

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

POSITIONS HELD

Duality Technologies, Inc., Newark, NJ and Tel Aviv, Israel (June. 2017 - present)

Co-Founder and CTO: Co-Founder of a leading encrypted computing start-up that is commercializing technologies that enables data science on encrypted data. Duality is currently spread across offices in Newark NJ and Tel Aviv Israel. Co-founders include a Turing award winner, MIT professor, former RSA data science executive and a venture capitalist. Duality is developing encrypted computing solutions for privacy-preserving analytics in regulated industries such as in the financial and healthcare industries. Duality investors include a major cybersecurity-focused VC fund and several high-net-worth individuals. Financial support also provided by NIH.

Seed and Series A investments of $20M from Intel Capital, Hearst Ventures and Team8. Series A led by Intel Capital.

In my role as CTO, I oversee all technical development, covering the spectrum of research to product development, deployment, integration and product support. I have a growing team of experienced world-class cryptographers, data scientists, systems engineers, architects, software engineers and programmers.

HomomorphicEncryption.org, (June. 2018 - present)

Co-Founder and Steering Committee Member: Co-Founder and steering committee member of an open industry consortium to standardize homomorphic encryption technologies across library developers and users. Co-founding members include Microsoft, IBM, Intel, Samsung, Duality Technologies, MIT, Seoul National University, NJIT and additional advanced technology organizations.

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

Winner of DARPA Young Faculty Award and DARPA Director's Fellowship

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, research professors, programmers, and graduate students.

Project achievements include:

- DARPA MARSHAL: Principal Investigator for a multi-year, multi-million dollar DARPA-funded R&D effort to optimize open-source compute-intensive workloads on military-relevant embedded systems. Project is resulting on deployment of PALISADE onto SOC- GPU- and FPGA-based embedded systems with transition to open source.
- 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. 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.

- Sloan Foundation REVET: Principal Investigator on a project funded by the Sloan Foundation to apply encrypted computing techniques in the social sciences. Partnered with the University of Michigan and MIT to develop and deploy encrypted computing techniques in an operational social science data science environment to analyze effectiveness of federal grantmaking at universities in the United States.
- 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 and IARPA HECTOR: 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 resulted in a first-ever domain-specific-language to make encrypted computing easier to use and deploy. Project also motivated a full $30M IARPA Program called HECTOR which I am now beginning to participate in.

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, and students. 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 external sponsorship and partnerships including with DARPA, IARPA, HSARPA, NSA, NSF, ARL and US Navy SPAWAR. Industry technology partners include Raytheon BBN Technologies, Perspecta Labs, Two Six Labs, Galois Inc., Cybernetica AS and LGS Innovations.

Avometric LLC, Maplewood, NJ (Aug. 2015 - present)

Founder: Founder of a boutique defense R&D consulting firm created to increase Technology Readiness Level (TRL) of DARPA-funded basic research, including for the transition of basic research results into operational military environments. Funded project activities include:

- SHARE: DARPA-funded project to mature and transition Proxy Re-Encryption technologies in the PALISADE library into multi-level security environments for multi-national military operations. Target transition user is in the US Special Forces community.
- AFRL SBIR: 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, Lattice-based Trapdoor, Attribute-Based 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 PALISDE 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, the Sloan Foundation, ONR and IARPA, and is contributing to project success on the DARPA MARSHAL, DARPA SafeWare, DARPA SHARE and IARPA HECTOR programs. Current developers, contributors and evaluators of the PALISADE library include NJIT, MIT, Sabanci University, Waseda University, WPI and UCSD from academia and Raytheon BBN, Perspecta Labs (formerly known as ACS/Vencore Labs), LGS Innovations, Galois Inc. and TwoSix 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-cluase BSD license in 2010 and has not been under active public development since then.

GRANTS AND CONTRACT AWARDS

- Sloan Foundation Crannog, co-PI. Duality Technologies Award: $350K, partnering with NumFocus and University of Michigan.
- IARPA Safe and Secure HECTOR subcontracted to Galois Inc., subcontract PI. NJIT Award: $2.1M. Selected for funding, currently in contracting. Period of Performance 2019-2023.
- ONR Human-AI Symbiosis for Agile Planning Subcontract co-PI, subcontract to UConn. NJIT award: $523K, ONR Grant 316317, Period of Performance 2018-2022.
- NIH SBIR GEARS, Duality Technologies Award: $150K, Principal Investigator, NIH Grant 1R43HG010123-01, Period of Performance 2018
- DARPA Young Faculty Award MARSHAL. NJIT award $950k, Principal Investigator. SPAWAR Contract N66001-17-1-4043. Period of Performance 2016-2020
- Sloan Foundation, REVET. NJIT Award $611k, Principal Investigator. Period of Performance 2017-2018
- 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
- IARPA Safe and Secure RAMPARTS Seedling Subcontracted to Galois, Inc. Subcontract PI. NJIT Award: $393K.
- PARAPET, NSA. Principal Investigator. NJIT Award: $298K. NSA grant H98230-15-1-0274.
- 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.
- 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.
- AFRL Information Directorate, Scalable Information Management Technology And Research (SCIMITAR). Raytheon BBN Technologies Award: $700K (approx.). AFRL contract award FA8750-12-C-0083
- META, DARPA STO. Contract award HR0011-10-C-0108, $2M (aprox.) (Tech Lead)
- International Crisis Early Warning System (ICEWS), DAPRA IPTO. AFRL/HECS contract FA8650-07-C-774, $6M (approx.). (Tech Lead)

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
      - Spring 2017. Rating: 3.13/4.00
      - Spring 2018. 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:
      - Fall 2016. Rating: 3.40/4.00
      - Fall 2017. Rating: 3.20/4.00
- **Introduction to Cryptography, NJIT CS 608.**
  - 3 credit-hour lecture course.
  - Course size: 36 students
  - Adopted this online video lecture course from a faculty member who separated from the department unexpectedly. Course focuses on introducing the major aspects of modern cryptography, including symmetric and public key cryptosystems. Focus is on algorithmic design that supports implementations, with supporting computational hardness introductions.
  - Course offerings:
    - Distance Offering:
      - Fall 2018, Spring 2019. Couse is currently ongoing

PUBLICATIONS

Journals

J1. Gür, K. D., Polyakov, Y., Rohloff, K., Ryan, G. W., Sajjadpour, H., and Savaş, E., "Practical Applications of Improved Gaussian Sampling for Trapdoor Lattices", Accepted for IEEE Transactions on Computers (IEEE TC), [https://eprint.iacr.org/2017/1254].

J2. Dai, W., Doröz, Y., Polyakov, Y., Rohloff, K., Sajjadpour, H., Savaş, E., and Sunar, B., "Implementation and Evaluation of a Lattice-Based Key-Policy ABE Scheme", IEEE Transactions on Information Forensics and Security (IEEE TIFS), 2018, Vol. 13, No. 5, pp. 1169-1184 [http://eprint.iacr.org/2017/601].

J3. 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).

J4. 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)

J5. 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).

J6. 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).

J7. 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.

J8. 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.

J9. 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.

J10. 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.

J11. 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.

J12. 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.

J13. Kurt Rohloff, Tae-Sic Yoo, Stéphane Lafortune. Deciding Coobservability is PSPACE-complete. IEEE Transactions of Automatic Control (IEEE TAC), 48:11. November, 2003

J14. 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

S1. Cousins, D. B., Di Crescenzo, G., Gür, K. D., King, K., Polyakov, Y., Rohloff, R., Ryan, G. W., and Savaş, E., "Implementing Conjunction Obfuscation under Entropic Ring LWE", 2018 IEEE Symposium on Security and Privacy (IEEE S&P), pp. 354-371 [https://eprint.iacr.org/2017/844].

S2. Gür, K. D., Polyakov, Y., Rohloff, K., Ryan, G. W., and Savaş, E., "Implementation and Evaluation of Improved Gaussian Sampling for Lattice Trapdoors", WAHC '18: 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography [http://eprint.iacr.org/2017/285].

S3. Di Crescenzo, G., Bahler, L., Coan, B. A., Rohloff, K., and Polyakov, Y.,"Intrusion-Resilient Classifier Approximation: From Wildcard Matching to Range Membership", TrustCom/BigDataSE 2018, pp. 1885-1890.

S4. Houle M.E., Oria V., Rohloff K.R., Wali A.M. (2018) LID-Fingerprint: A Local Intrinsic Dimensionality-Based Fingerprinting Method. In: Marchand-Maillet S., Silva Y., Chávez E. (eds) Similarity Search and Applications. SISAP 2018. Lecture Notes in Computer Science, vol 11223. Springer, Cham

S5. Bahler, L., Di Crescenzo, G., Polyakov, Y., Rohloff, R., and Cousins, D. B., "Practical Implementation of Lattice-Based Program Obfuscators for Point Functions", 2017 International Conference on High Performance Computing & Simulation (HPCS 2017), 17-21 July 2017.

S6. Gupta, A. D., Polyakov, Y., Rohloff, K., and Ryan, G., "Securely Sharing Encrypted Medical Information", IEEE CHASE 2016, 27-29 June 2016.

S7. Di Crescenzo, G., Bahler, L., Coan, B., Polyakov, Y., and Rohloff, K., and Cousins, D., "Practical Implementations of Program Obfuscators for Point Functions", 2016 International Conference on High Performance Computing & Simulation (HPCS 2016), 18-22 July 2016.

S8. Gupta, A. D., Polyakov, Y., and Rohloff, K., "Secure Access Delegation of Encrypted Medical Information", 10th International Symposium on Medical Information and Communication Technology (ISMICT'16), Worcester, MA, 20-23 March 2016.

S9. Rohloff, K. and Polyakov, Y., "An End-to-End Security Architecture to Collect, Process and Share Wearable Medical Device Data", 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), Boston, MA, 14-17 October 2015, pp. 615-620.

S10. 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

S11. 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.

S12. 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.

S13. 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.

S14. 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.

S15. 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.

S16. 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.

S17. 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.

S18. Kurt Rohloff, Jeffrey Cleveland, Joseph Loyall, Timothy Blocher "SCIMITAR: Scalable Stream-Processing for Sensor Information Brokering." Military Communications Conference (MILCOM), Nov. 18-20, 2013.

S19. 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.

S20. 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.

S21. Kurt Rohloff "Bounded Sensor Failure Tolerant Supervisory Control." 11th International Workshop on Discrete-Event Systems (WODES), Oct. 3-5, 2012.

S22. 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.

S23. 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.

S24. 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.

S25. 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.

S26. 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

S27. 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.

S28. 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.

S29. 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.

S30. 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.

S31. 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.

S32. 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.

S33. Kurt Rohloff. "Automated Discovery and Modeling Of Sequential Patterns Preceding Events of Interest." ModSim World, Oct. 2009.

S34. Kurt Rohloff and Paul Rubel. "Discovering Automated Sequential Patterns the Precede Outbreaks of Socio-Political Violence." HSCB Focus 2010, August, 2009.

S35. 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.

S36. Kurt Rohloff and Wayne Thornton. "A Knowledge Environment for Social Science Exploration." Human Behavior-Computational Intelligence Modeling Conference, June 2009.

S37. 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.

S38. 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.

S39. 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

S40. 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.

S41. 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.

S42. Kurt Rohloff. "Directions for Cost-Effective Certification of High-Assurance Cyber Physical Systems." Fourth Annual Carnegie Mellon Conference on the Electricity Industry, March 2008.

S43. 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

S44. 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

S45. 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.

S46. 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.

S47. 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.

S48. 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.

S49. 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.

S50. 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.

S51. 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.

S52. 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.

S53. 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.

S54. 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.

S55. Kurt Rohloff, The Diagnosis of Failures via the Combination of Distributed Observations, Mediterranean Conference on Decision and Control, 2005.

S56. Kurt Rohloff, Jan H. van Schuppen. Approximating Minimal Communicated Event Sets for Decentralized Supervisory Control, IFAC World Congress, 2005.

S57. Kurt Rohloff, Tansu Alpcan, Tamer Başar. A Discrete-Event Systems Model for Congestion Control, IFAC World Congress, 2005.

S58. 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.

S59. 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.)

S60. Kurt Rohloff, Stéphane Lafortune. Symmetry Reductions for a Class of Modular Discrete-Event Systems, Conf. on Decision and Control, 2004.

S61. Kurt Rohloff, Stéphane Lafortune. The Control and Verification of Similar Agents Operating in a Broadcast Network, Conf. on Decision and Control, 2003.

S62. Kurt Rohloff, Stéphane Lafortune. Supervisor Existence for Modular Discrete-Event Systems, Proc. of the 2nd IFAC Conf. on Control Systems Design, 2003.

S63. Kurt Rohloff, Stéphane Lafortune. Recent Results on Computational Issues in Supervisory Control, Proc. of the ATPN-Workshop Discrete Event Systems Control, 2003.

S64. 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. 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

T2. Kurt Rohloff, Stéphane Lafortune. Deciding Coobservability is PSPACE-complete, University of Michigan EECS Technical Report CGR-03-06

T3. 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

T4. Kurt Rohloff, Stéphane Lafortune. Symmetry Reductions for a Class of Distributed Discrete-Event Systems, University of Michigan EECS Technical Report CGR-04-02

T5. 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. “Cloud computing for Scalability: The SHARD Triple-Store.” Cambridge SemWeb MeetUp, January 9, 2011.

S11. Kurt Rohloff. “Cloud computing for Scalability: The SHARD Triple-Store.” SemWeb MeetUp Webcast, January 9, 2011.

S12. Kurt Rohloff. “SHARD: Cloud-Computing for a Scalable Semantic Web.” Tufts University Computer Science Colloquium. September 16, 2010.

S13. Kurt Rohloff. “SHARD: Storing and Querying Large-Scale SemWeb Data.” HadoopWorld, 2010.

S14. Kurt Rohloff. “Cloud- and Cluster-Computing Technologies for the Semantic Web.” Semantic Technology Conference, 2010.

PATENTS

P1. Kurt Rohloff, Richard Schantz and David Bruce Cousins. “Method for Secure Symbol Comparison” U.S. Patent No. 9,893,880. February 13, 2018

P2. Kurt Rohloff " System and method for merging encryption data without sharing a private key" U.S. Patent No. 9,628,450. April 18, 2017.

P3. Kurt Rohloff and David Bruce Cousins. “System and method for encoding encrypted data for further processing” U.S. Patent No. 9,628,266. April 18, 2017.

P4. Kurt Rohloff "System and method to merge encrypted signals in distributed communication system." U.S. Patent No. 9,461,974. October 4, 2016.

P5. 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

P6. Kurt Rohloff. “System and method for operating on streaming encrypted data.” U.S. Patent No. 9,338,144. May 10 2016.

P7. Kurt Rohloff. “System and method for merging encryption data using circular encryption key switching.” U.S. Patent No. 9,325,671. April 26, 2016.

P8. 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. " DEVICE, SYSTEM AND METHOD FOR FAST AND SECURE PROXY RE-ENCRYPTION." United States Patent Application 20170155628. Filed 2017.

A2. Kurt Rohloff and David Bruce Cousins. " SYSTEM AND METHOD FOR ENCODING ENCRYPTED DATA FOR FURTHER PROCESSING." United States Patent Application 20170078086. Filed 2017.

A3. 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.

A4. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD TO MERGE ENCRYPTED SIGNALS IN DISTRIBUTED COMMUNICATION SYSTEM." United States Patent Application 20150249650. Filed 2014.

A5. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD TO MERGE ENCRYPTED SIGNALS IN DISTRIBUTED COMMUNICATION SYSTEM." United States Patent Application 20150249649. Filed 2014.

A6. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MIXING VOIP STREAMING DATA FOR ENCRYPTED PROCESSING." United States Patent Application 20150244516. Filed 2014.

A7. Kurt Rohloff and David Bruce Cousins. "SYSTEM AND METHOD FOR MIXING VOIP STREAMING DATA FOR ENCRYPTED PROCESSING." United States Patent Application 20150237020. Filed 2014.

A8. 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.

A9. Kurt Rohloff, David Bruce Cousins and Richard Schantz. "METHOD FOR SECURE SYMBOL COMPARISON." United States Patent Application 20140233728. Filed 2013.

A10. Kurt Rohloff, David Bruce Cousins and Richard Schantz. "METHOD FOR SECURE SUBSTRING SEARCH." United States Patent Application 20140233727. Filed 2013.

ACADEMIC AWARDS AND HONORS

- DARPA Young Faculty Award, 2017
- 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, Finished ABD)
- Gerard Ryan, NJIT PhD, Expected Spring 2019.
- Cavidan Yakupoglu, NJIT PhD, Expected Spring 2020

Masters Thesis Students

- Kamil Doruk Gur, NJIT MS, Expected Spring 2019
- 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

- Francesco Primerano, NJIT, Spring 2019, Student Programmer on ONR AI project.
- 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:

- ACM (2018-present)
- IEEE (1997-present)
- AAAI (2009-2010)

NJIT Service

- NJIT Institute Intellectual Policy review Board 2016-present
- NJIT Faculty Research Advisory Board, 2014-present
- 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:
    - HomomorphicEncryption.org Standards meeting, 2017-2019
    - Workshop on Encrypted Computing and Applied Homomorphic Cryptography (WAHC), 2015-2019
    - 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

- **NJIT News** "Computer Science Professor's Startup Attracts Millions in Investment From Industry Leaders" December 5, 2018
- **Silicon Republic** "Kurt Rohloff of Duality Technologies on the future of encryption" November 14, 2018
- **Fortune** "Walmart, Microsoft, AT&T-Backed Foundry Invests Millions in Encryption Pioneer" November 13, 2018
- **TAPintoNewark** "Safety in Numbers: Computer Scientist Races to Develop Unhackable Code to Protect Everyone's Data" July 13, 2018
- **NJBiz** "Cybersecurity: Plan for the worst, and expect to be hacked despite all best efforts", March 19, 2018
- **The Chronicle of Higher Education** "2 New Threats Highlight Human-Factor Gaps in Cybersecurity Research" January 12, 2018
- **Senator Ron Wyden Official Website** "Wyden, Rubio, Warner Introduce 'Student Right to Know Before You Go Act' to Empower Students as Consumers and Showcase New Privacy-Protecting Technology" Nov 29, 2017
- **NJTV News** "After Equifax breach, how worried should you be about your personal information?" Sept 12, 2017.
- **TechNews** "新的一年, 手機可能曝露在不安全中", Jan. 5, 2016
- **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
- **Innovation New Jersey** "A First for NJIT: Computer Science Professor Dr. Kurt Rohloff Wins DARPA Young Faculty Award" October 5, 2017
- **SecurityLab.ru** "DARPA создаст способы борьбы с реверс-инжинирингом программ", Sept 17, 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
- **Voice of America** "Encryption Debate Comes Out of the Shadows", July 13, 2015
- **CIO** "How to Overcome Roadblocks Facing the Security of Embedded Medical Devices", June 30, 2015
- **Federal Times** "OPM Breach a Failure on Encryption, Detection", June 19, 2015
- **USA Today** "Senate Bill Would Help Thwart Hackers, Expert Says", June 9, 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
- **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