Michael Thomas Kurdziel, Ph.D.

michael.kurdziel2001@gmail.com

585-594-4374

Leadership - Innovation - Execution

EDUCATION	**Ph.D.** Electrical Engineering, State University of New York at Buffalo, 2001 **M.S.** Electrical and Computer Engineering, State University of New York at Buffalo, 1988 **B.S.** Electrical and Computer Engineering, State University of New York at Buffalo, 1986
QUALIFICATIONS	• Recognized as a published industry authority in the Tactical Information Assurance field. • Technical expertise in the area of secure communications systems design. This includes the design of ConOps level communication, encryption, key management and authentication systems, Type 1 algorithm implementation, anti-tamper scheme analysis and implementation, cryptographic randomizer design and evaluation, zeroization scheme analysis and implementation, design for FIPS-140-2 certification and Type 1 security analysis and IAD certification. • Other responsibilities include consultation on architecture development for the company's line of Type 3 and Type 4 encryption devices and preparing and presenting training courses for the technical staff, sales team and for external customers. • Contributed as principal algorithm architect for the MK-128 and MK-256 encryption algorithms used in the Citadel ™ and Citadel II™ Encryption Devices. The devices are Harris Corporation's primary encryption solution for non-Type 1 applications. • PMI certified Project Management Professional since 2013. • Professional Engineer (License No. 069432) in the State of New York since 1992.
EXPERIENCE 2012 to present	**Rochester Institute of Technology, Rochester, NY** • **Adjunct Professor** o Computer Science Department ▪ CSCI 462, Introduction to Cryptography, Fall 2015 to present o Computer Engineering Department ▪ CMPE 661, Hardware and Software Design for Cryptographic Applications, Spring 2014 to present ▪ EECC 0306-381, Applied Programming (Numerical Methods) Spring 2012, Spring 2013
2020 to present 2017 to present 2012 to 2017	**L3Harris Technologies Inc., Communication Systems Segment,** Rochester, NY • **L3Harris Technologies Fellow – Cryptography, Information Assurance and Cyber Security** • **Director, Chief Engineering – Systems and Technology Group** • **Senior Engineering Manager of the Core Networking and Network Security Group** o Responsibilities include supervision of a team of 25 Core Networking and Embedded Software experts, planning and tracking the simultaneous execution of multiple Core Networking and Network Security programs. o Established an initiative to achieve platform networking service commonality across multiple radio product lines.
2009 to present 2011 to present 2011 to present	• **Supervisor** of several funded L3Harris University Relations Projects with the Rochester Institute of Technology • **Chairman** of Harris Communications Systems Segment, Intellectual Property Management Committee • **Chairman** of Harris Communications Systems Segment Information Assurance Working Group

2009 to 0012	• **Senior Engineering Manager Defense Systems Architecture (DSA) Group** o Responsibilities include leader of a division-wide initiative to create a "Center of Excellence" for tactical communications systems design, establishment of a CMMI qualified Systems Development Process, Supervision of a team of Systems Architects.
2001 to 2009	• **Senior Engineering Manager Communications Security Products (CSP) Group** o Responsibilities include supervision of a team of 70 highly skilled and experienced COMSEC engineers, business development activities as well as planning and tracking the simultaneous execution of multiple programs.
1992 to 2001	• **Various technical roles of increasing responsibility** o **Principal Technical Specialist and Chief Cryptographer** on the specification and design of non-Type 1 encryption solutions for Military & Government applications. ▪ Responsibilities also include the ongoing technical support of business development and sales opportunities. o **Project Leader and Principal Hardware Engineer** on a program to develop a line of programmable encryption modules for a variety of applications. The product features a programmable platform capable of supporting a range of customer specified symmetric encryption algorithms. Public Key Management functions are also provided using the Diffie-Hellman Key Exchange algorithm. o **Project Leader and Lead Hardware Engineer** on a program to develop a line of non-Type-1 encryption ASICs. o **Member of Technical Staff** for the development of two proprietary Type 1 COMSEC ASIC encryption/decryption device design projects
1988 to 1992	**Electronetics Corporation, Buffalo, NY** • **Project Leader and Principal Electronic Design Engineer** for the company's proprietary line of commercial products, a microprocessor based instrument designed to create, sustain and control an RF glow discharge for industrial cleaning. • **Design Engineer** - provided technical support on classified defense department program. Primary area of performance consisted of DSP design and simulation. • **Design Engineer** - provided technical support on contract for the design and development of FASCAM Land Mine Automatic Test System.
PROFESSIONAL ACTIVITIES	• IEEE MILCOM Conference, Technical Program Chairman, 2019. • IEEE MILCOM Conference Co-Chair, Unclassified Technical Panels Program, 2018. • IEEE MILCOM Conference Vice Chair, Unclassified Technical Program, 2016, 2017. • IEEE MILCOM Conference Track Co-Chairman, Cyber Security and Trusted Computing, 2015. • IEEE MILCOM Conference Track Co-Chairman, Services and Applications, 2012. • IEEE MILCOM Conference Session Chairman and Technical Program Committee Member, 2003 - present. • Director, Rochester Engineering Society - Board of Directors, 2019 – Present. • Industrial Advisory Board Member for the Rochester Institute of Technology, Computer Engineering, 2008 – Present. • Industrial Advisory Board Member for SUNY at Buffalo, Computer Science and Engineering, 2013 – Present. • Keynote speaker for the Finger Lakes Chapter of INCOSE, 2013. o "Application of System Engineering Principles to Close Cyber Security Threats" • Evaluator for NSERC's Collaborative Researcher and Development (CRD) Grants, 2013. • Presenter for the Rochester Institute of Technology, CS4HS@RIT Workshop, June 2010, June 2011, June 2012. • Tactical Radio Co-Chairman of the International Interconnectivity Working Group (I-ICWG) for development of radio aspects of the Secure Communication Interoperability Protocol (SCIP) Specification, 2005 - 2013. • Program committee member for the IEEE SRDS09 Workshop on Embedded Systems and Communications Security, Niagara Falls, September 2009. • Program committee member for the International Conference and Workshop on Cyber Security, Cyber Crime and Cyber Forensics, Kochi, India, August 2009. • Keynote speaker for Northeast Collegiate Cyber Defense Competition at Rochester Institute of Technology,

	March 2009. • Presenter at the Rochester Institute of Technology, Electrical Engineering Distinguished Speaker Series, February 2009.
JOURNAL PUBLICATIONS	• P. Bajorski, M. Kurdziel, "A Markov-Chain-Based Model for Group Message Distribution in Connected Networks," International Journal of Data Analytics (IJDA), Issue 1(2), 2020. • P. Bajorski, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, C. Wood, "Stochastic Analysis and Modeling of a Tree-Based Group Key Distribution Method in Tactical Wireless Networks", Journal of Telecommunications System Management, Volume 3, Issue 115, 2014. • M. Kurdziel, M. Łukowiak, M. Sanfilippo, "Minimizing performance overhead in memory encryption", Journal of Cryptographic Engineering, Springer, Volume 3, Issue 2, Page 129-138, 2013.
CONFERENCE PUBLICATIONS (Peer Reviewed)	• C. Tinker, K. Millar, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, "Exploring the Application of Homomorphic Encryption to a Cross Domain Solution", Proc. IEEE, Mil. Comm. Conf., November 2019. • P. Bajorski, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, "Customization Modes for the Harris MK-3 Authenticated Encryption Algorithm", Proc. IEEE, Mil. Comm. Conf., October 2018. • P. Bajorski, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, "Array-Based Statistical Analysis of the MK-3 Authenticated Encryption Scheme", Proc. IEEE, Mil. Comm. Conf., October 2018. • G. Werner, S. Farris, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, "Implementing Authenticated Encryption Algorithm MK-3 on FPGA", Proc. IEEE, Mil. Comm. Conf., November 2016. • M. Kurdziel, M. Łukowiak, Radziszowski, G. Werner S. Farris, A. Kaminsky, "Fully Parallel Implementation of the MK-3 Authenticated Encryption Algorithm on FPGA", New York Cyber Security and Engineering Technology Association (NYSETA) Conf., Rochester, NY, October 2015. • P. Bajorski, C. Wood, M. Kurdziel, "General Stochastic Model for Tree-based Message Distribution in Wireless Networks", Proc. Simulation, Modeling, Mathematical Statistics (SMMS2015) Conf., Chiang Mai, Thailand, November 2015. ISBN: 978-1-60595-112-6. • M. Kelly, A. Kaminsky, M. Kurdziel, M. Łukowiak, S. Radziszowski, "Customizable Sponge-Based Authenticated Encryption Using 16-bit S-boxes'", Proc. IEEE, Mil. Comm. Conf., October 2015. • M. Kurdziel, J. Alvermann, "Information Security Trades In Tactical Wireless Networks", Proc. SPIE 9497, Mobile Multimedia/Image Processing, Security, and Applications, 2015. • M. Kurdziel, "Cyber Threat Model for Tactical Radio Networks", Proc. SPIE 9103, Wireless Sensing, Localization, and Processing IX, 910305, May 2014. • A. Fitzgerald, M. Łukowiak, M. Kurdziel, C. Mackey, K. Smith Jr, B. Boorman, D. Harris, W. Skiba, "FPGA-Based, Multi-Processor HW-SW System for Single-Chip Crypto Applications", Proc. IEEE, Mil. Comm. Conf., October 2010. • M. Kurdziel, A. Kaminsky, S. Radziszowski, "An Overview of Cryptanalysis Research for the Advanced Encryption Standard", Proc. IEEE, Mil. Comm. Conf., October 2010. • M. Kurdziel, J. Alvermann, W. Furman, "The Secure Communication Interoperability Protocol (SCIP) Over a VHF/UHF Radio Channel", Proc. IEEE, Mil. Comm. Conf., October 2008. • B. Boorman, C. Mackey, M. Kurdziel, "Scalable Hardware Architecture to Support Applications of the HAIPE 3.1 Standard", Proc. IEEE, Mil. Comm. Conf., October 2007. • M. Kurdziel, J. Alvermann, W. Furman, "The Secure Communication Interoperability Protocol (SCIP) Over an HF Radio Channel", Proc. IEEE, Mil. Comm. Conf., October 2006. • J. Alvermann, M. Kurdziel, W. Furman, "Simulation Studies of SCIP Over HF", International Interconnectivity Working Group, June 2006. • M. Kurdziel, J. Beane, J. Fitton, "An SCA Security Supplement Compliant Radio Architecture", Proc. IEEE, Mil. Comm. Conf., October 2005. • M. Kurdziel, "Communications Security Alternatives For Military Sensor Net Telemetry Links", IEEE Workshop on Comm. and Networking, November 2004. • M. Kurdziel, R. Clements, G. Dennis, "Customizable Cryptographic Architecture for Government & Military Communications Applications", Proc. IEEE, Mil. Comm. Conf., October 2004. • M. Kurdziel, W. Furman, "Scalar Quantization of Images for HF Transmission", NATO NC3A Ad-Hoc Working Group 3 (AHWG/3), The Hague, Netherlands, August 2004. • M. Kurdziel, G. Dennis, "An AES Variant for Military and Government COMSEC Applications", Proc. IEEE, Mil. Comm. Conf., October 2003. • M. Kurdziel, W. Furman, "Image Compression and Transmission for HF Radio Systems", Proc. IEEE, Mil. Comm. Conf., Oct. 2002.

	• M. Kurdziel, J. Fitton, “Baseline Requirements for Government & Military Encryption Algorithms”, Proc. IEEE, Mil. Comm. Conf., October 2002. • M. Kurdziel, R. Clements, “Harris Customizable Cryptographic Architecture”, Proc. IEEE, Mil. Comm. Conf., pp. 1033-1037, October 1998. • M. Kurdziel, R. Acharya, “A New Technique for Adaptive Scalar Quantization of Image Sub-Band Coefficients”, Proc. IEEE, Mil. Comm. Conf., pp. 350-354, October 1998.
US PATENTS	• 10,666,437: Customizable encryption/decryption algorithm, 2020 • 9,438,416: Customizable encryption algorithm based on a sponge construction with authenticated and non-authenticated modes of operation, 2016. • 8,873,759 Electronic key management using PKI to support group key establishment in the tactical Environment. 2014. • 8,719,593 Secure processing device with keystream cache and related methods, 2014. • 8,218,574 Scalable packet analyzer and related method, 2012. • 8,165,305 Enhanced relational database security through encryption of table indices, 2012. • 7,979,714 Authentication and access control device, 2011. • 7,672,455 Method and apparatus for data encryption, 2010. • 7,613,297 Method and apparatus for data encryption, 2009. • 7,613,295 Cryptographic device and associated methods, 2009. • 7,606,368 Method and apparatus for data encryption, 2009. • 7,599,490 Method and apparatus for data encryption, 2009. • 7,293,054 Random number source and associated methods, 2007. • 7,251,326 Method and apparatus for data encryption, 2007. • 7,212,638 Wireless cryptographic fill system and method, 2007. • 6,108,421 Method and apparatus for data encryption, 2000. • 5,692,098 Real-time Mozer phase recoding using a neural-network for speech compression, 1997.
THESIS COMMITTEES	• C. Tinker, “Exploring the Application of Homomorphic Encryption for a Cross Domain Solution”, MS Thesis, Rochester Institute of Technology, August 2018. • M. Kelly, ‘’Design and Cryptanalysis of Authenticated Encryption Constructions”, MS Thesis, Rochester Institute of Technology, May 2014. • C. Wood, “Large Substitution Boxes with Efficient Implementations”, MS Thesis, Rochester Institute of Technology, September 2013. • M. Hogan, “Towards Flexible Hardware/Software Encoding using H.264”, MS Thesis, Rochester Institute of Technology, September 2011. • M. Sanfilippo, “Extremely Low Overhead Off-Chip Memory Encryption”, MS Thesis, Rochester Institute of Technology, August 2011. • T. Sperr, “Investigating Low-Bit Rate, Low-Complexity H.264 Region of Interest Techniques in Error-Prone Environments”, MS Thesis, Rochester Institute of Technology, June 2011. • A. Fitzgerald, “Design and Analysis of an FPGA-based, Multi-processor HW-SW System for SCC Applications”, MS Thesis Rochester Institute of Technology, May 2010. • K. Smith Jr, “The Feasibility of Power Analysis Attacks on FPGA Implementations of AES”, MS Thesis Rochester Institute of Technology, August 2009. • T. VanAmeron, “Implementing Efficient 384-Bit NIST Elliptic Curve Over Prime Fields on an ARM946E”, MS Thesis, Rochester Institute of Technology, April 2008.
AWARDS	• RIPLA Inventor of the Year, 2019. • Harris Technology Innovation Award, 2019. • Nominee, RIPLA Inventor of the Year, 2017. • Harris Industry Recognition Award, 2012, 2017. • Harris Golden Quill Award for Excellence in Publications, 2005, 2006, 2009, 2015, 2016, 2018, 2019. • Harris Next Level Award, 2001, 2014. • Harris Excellence Award, 2005, 2014. • Pakistan Signals Establishment Sword, 2009.

AFFILIATIONS	Institute of Electrical and Electronic Engineers, AFCEA, Mensa, Program Management Institute
SECURITY CLEARNCE	• Top Secret - Defense Investigative Services, 1989 • Top Secret/SCI - Defense Investigative Services, 2008 • Top Secret – Central Intelligence Agency, 1995 • Secret – Singapore Defence Services Organization, 2001