Curriculum Vitae
Mike V. D. Burmester
2017

General Information

University address:	Computer Science College of Arts and Sciences Love Building 0268 Florida State University Tallahassee, Florida 32306-4530 Phone: 8506446410; Fax: 8506440058
E-mail address:	burmester@cs.fsu.edu
Web site:	http://www.cs.fsu.edu/~burmeste/

Professional Preparation

1966	Dott. Mat., University of Rome "La Sapienza", Italy. Major: Mathematics. Supervisor: B. Segre. Summa cum laude.
1961	BA, University of Athens, Greece. Major: Mathematics. Supervisor: K. Kappos.

Professional Experience

2006–present	Courtesy Professor, Computer and Information Sciences (CIS), Florida A&M University.
2000–present	Professor, Florida State University.
1996–2000	Reader, Information Security Group, Royal Holloway, University of London.
1966–1996	Lecturer, Mathematics, Royal Holloway, University of London.
1974–1975	Associate Professor, Illinois State University, Normal, Illinois.
1967–1968	Assistant Professor, Computer Science, University of Illinois, Chicago Circle, Chicago.

Visiting Professorship(s)

2007	University of Calgary, Canada.
2001	George Mason University, Fairfax, VA.
2000	Queensland University of Technology, Brisbane, Australia.
1999	Japan Advanced Institute of Science and Technology (JAIST), Kanasawa, Japan.
1997–1999	University of Piraeus, Athens, Greece.
1995–1997	Adjunct Associate Professor, University of Wisconsin, Milwaukee.
1992	Visiting Associate Professor, University of Wisconsin, Milwaukee.

Fellowship(s)

Institute of Mathematics and its Applications (FIMA) (1995–2009).
Hellenic Mathematical Society (1990–2005).

Current Membership in Professional Organizations

Cyber-Physical Systems Virtual Organization, NSF (CPS-VO)
IEEE Computer Society, Senior Member
IFIP WG 11.14 (Secure Service Engineering)
Institute for Systems and Technologies of Information, Control and Communication (INSTICC)
Institute of Electronics, Information and Communication Engineers (IEICE)
International Association of Cryptologic Research (IACR)

Research and Original Creative Work

Program of Research and/or Focus of Original Creative Work

Program Area: Cyber Security, Information Assurance
Focus Areas: (a) Pervasive/Ubiquitous systems, (b) Cyber Physical Systems.
Focus Subareas: Cryptography, Network Security, Internet of Things (IOT), Sensor networks, RFID, Trust Management, Privacy/Uncoercibility, Watermarking/Fingerprinting, Information Hiding.

Publications

Refereed Journal Articles

Burmester, M., Munilla, J., Ortiz, A., & Caballero-Gil, P. (2017). An RFID-Based Smart Structure for the Supply Chain: Resilient Scanning Proofs and Ownership Transfer with Positive Secrecy Capacity Channels. *Sensors (JRC-IF:2.67), 17(7),* 1562. doi:10.3390/s17071562

Kotzanikolaou, P., Chatzisofroniou, G., & Burmester, M. (2017). Broadcast anonymous routing (BAR): scalable real-time anonymous communication. *Int. J. Inf. Sec. (JCR-IF:1.95), 16(3),* 313-326. doi:10.1007/s10207-016-0318-0

Álvarez-Díaz, N., Caballero-Gil, P., & Burmester, M. (2017). A Luggage Control System based on NFC and Homomorphic Cryptography. *Mobile Information Systems (JCR-IF 1.5), 2017*, 18. doi:10.1155/2017/2095161

Burmester, M., & Munilla, J. (2017). Performance Analysis of LDPC based RFID Group Coding. *IEEE Trans. Automation Science and Engineering (JRC-IF:2.7), 14(1),* 398-402. doi:DOI: 10.1109/TASE.2016.2604339

Munilla, J., Burmester, M. V., A Peinado, A., Yang, G., & Susilo, W. (2016). RFID Ownership Transfer with Positive Secrecy Capacity Channels. *Sensors (JRC-IF 2.03), 17(1),* 53. doi:doi:10.3390/s17010053

Munilla, J., Burmester, M., & Peinado, A. (2016). Attacks on Ownership Transfer for Multi-Tag Multi-Owner Passive RFID Environments. *Computer Communications, Elsevier (JRC-IF:2.1), 88*, 84--88. doi:doi:10.1016/j.comcom.2016.05.007

Burmester, M., & Munilla, J. (2016). Tag Memory-Erasure Tradeoff of RFID Grouping Codes. *IEEE Communications Letters (JRC-IF:1.3), 20(6),* 1144-1147. Retrieved from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7440837 doi:10.1109/LCOMM.2016.2546857

Liu, X., Burmester, M., Wilder, F., Redwood, W. O., & Butler, J. (2014). Zero-Day Vulnerabilities: What to do when it's too late to prevent an attack. *Marine Safety and Security Council, 71 (4),* 28--33.

Burmester, M., & Munilla, J. (2014). Pre vs Post State Update: Trading Privacy for Availability in RFID. *IEEE Wireless Communications Letters (JRC-IF:1.3), 3,* 317-320. doi:10.1109/WCL.2014

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2012). Modeling security in cyber physical systems. *Int. J. Critical Infrastructure Protection, Elsevier, 5(3-4),* 118-126.

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2012). Secure and Privacy-preserving, Timed Vehicular Communication. *Int. J. Ad Hoc and Ubiquitous Computing, Inderscience, 10(4),* 219-229.

Kotzanikolaou, P., Avramidis, A., Douligeris, C., & Burmester, M. (2012). Chord-PKI: A distributed trust infrastructure based on P2P networks. *Computer Networks, 56(1),* 378-398.

Burmester, M., & Munilla, J. (2011). Lightweight RFID authentication with forward and backward security. *ACM Trans. Inf. Syst. Secur, 14(1),* 11 pages.

Bhattacharya, B., Burmester, M., Hu, Y., Kranakis, E., Shi, Q., & Wiese, A. (2009). Optimal movement of mobile sensors for barrier coverage of a planar region. *Theoretical Computer Science, 410(52),* 5515-5528.

Burmester, M., & De Medeiros, B. (2009). On the Security of Route Discovery in MANETs. *IEEE Trans. Mobile Computing, 8(9),* 1180-1188.

Burmester, M., Van Le, T., De Medeiros, B., & Tsudik, G. (2009). Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. *ACM Trans. Inf. Syst. Sec, 12(4),* Article 21:1-33.

Burmester, M., Van Le, T., De Medeiros, B., & Tsudik, G. (2009). Universally Composable RFID Identification and Authentication Protocols. *ACM Trans. Inf. Syst. Secur, 12(4),* 33 pages.

Burmester, M., De Medeiros, B., & Motta, R. (2008). Anonymous RFID Authentication with Constant Key-Lookup. *Int. J. Applied Cryptography, 1(2),* 79-90.

Burmester, M., van Le, T., & Yasinsac, A. (2007). Adaptive Gossip Protocols: Managing security and redundancy in dense Ad Hoc networks. *J. Ad hoc Networks, Elsevier, 5(3),* 313-323.

Burmester, M., & Desmedt, Y. (2005). A Secure and Scalable Group Key Exchange System. *Inf. Processing Letters, Elsevier, 94(3),* 137-143.

Burmester, M., Henry, P., & Kermes, L. (2005). Tracking Cyberstalkers: a cryptographic approach. *ACM SIGCAS Computers and Society, 35(3),* 16 pages.

Yasinsac, A., & Burmester, M. (2005). Centers of Excellence: A case study. *Security & Privacy, IEEE Computer Society, 3(1),* 62-65.

Burmester, M., & Desmedt, Y. (2004). Is hierarchical public-key certification the next target for hackers? *Communications of the ACM, 47(8),* 68-74.

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2004). Uncoercible e-Bidding Games. *Electronic Commerce Research, Kluwer Academic Publishers, 4(1-20),* 113-125.

Burmester, M., & Van Le, T. (2004). Attack on the Sebé, Domingo-Ferrer and Herrera-Joancomarti fingerprinting schemes. *Electronics Letters, Institute of Engineering and Technology, 40(2),* p. 172.

Burmester, M., & Yasinsac, A. (2004). Trust infrastructures for wireless mobile networks. *WSAES Transactions on Communications, 3(1),* 377-381.

Burmester, M., Desmedt, Y., Mambo, M., & Okamoto, E. (2002). Formal model of ordered multi-party cryptography and its concrete examples. *Trans. Fund. of Electronics, Communications and Computer Sciences, Institute of Electronics, Information and Communication Engineers (IEICE), E85-A(3),* 346-357.

Kotzanikolaou, P., Burmester, M., Chrissikopoulos, V., & Douligeris, D. (2002). Role based access control policies in the mobile agent paradigm. *Informatik Forum Journal, Special issue on Mobile Agent Technology, 14(2),* 62-69.

Beimel, A., Burmester, M., Desmedt, Y., & Kushilevitz, E. (2000). Computing Functions of a Shared Secret. *SIAM J. of Discrete Math, 13(3),* 324-345.

Burmester, M., Desmedt, Y., Alexandris, N., & Chrissikopoulos, V. (2000). Secure Linking of Customers, Shops and Banks in Electronic Commerce. *Security on the Web, Future Generation Computer Systems, Elsevier Science B.V, 16,* 393-401.

Wang, Y., Desmedt, Y., & Burmester, M. (2000). Models For Dependable Computation with Multiple Inputs and Some Hardness Results. *Fundamenta Informaticae, 42(1),* 61-73.

Burmester, M., Desmedt, Y. G., Itoh, T., Sakurai, K., & Shizuya, H. (1999). Divertible and subliminal-free zero-knowledge proofs of languages. *J. of Cryptology, Springer-Verlag, Berlin, 12(3),* 197-223.

Burmester, M., & Desmedt, Y. (1998). Secure Communication in an Unknown Network with Byzantine Faults. *Electronics Letters, Institute of Engineering and Technology, 34(8),* 741-742.

Burmester, M., Desmedt, Y., Piper, F. C., & Walker, M. (1997). A general zero-knowledge scheme. *Designs, Codes and Cryptography, 12(1),* 13-37.

Burmester, M., Desmedt, Y., & Yung, M. (1993). Canali "subliminal-free": Una soluzione verso canali "covert-free". *Rivista di Informatica, XX(1),* 5-14.

Burmester, M. (1992). An almost-constant round interactive zero-knowledge proof. *Information Processing Letters, 42(2),* 81-87.

Burmester, M., Desmedt, Y., & Beth, T. (1992). Efficient zero-knowledge identification schemes for smart cards. *The Computer Journal, Special issue on Safety and Security, 35(1),* 21-29.

Burmester, M., Chrissikopoulos, V., & Alexandris, N. (1992). Security of smart cards. *Mathematical Reviews of the Hellenic Mathematical Society, 38,* 72-84.

Burmester, M. (1991). Comments on the cryptanalysis of public key distribution systems. *Electronics Letters, Institute of Engineering and Technology, IEE 27,* p. 2042.

Burmester, M., Chrissikopoulos, V., & Alexandris, N. (1989). The structure and complexity of zero-knowledge proofs. *Bulletin of the Hellenic Mathematical Society, 30,* 1-20.

Burmester, M. V. D., & Desmedt, Y. G. (1989). Remarks on the soundness of proofs. *Electronics Letters, Institute of Engineering and Technology, 25,* 1509-1511.

Burmester, M., Chrissikopoulos, V., & Alexandris, N. (1989). Minimum knowledge systems. *Mathematical Reviews of the Hellenic Mathematical Society, 36,* 1-8.

Burmester, M. V. D., & Exarchakos, T. (1988). The function g(x) for which |A(G)|p ≥ ph whenever |G| ≥ pg(h), G a finite group. *Bulletin of the Hellenic Mathematical Society, 29,* 27-44.

Burmester, M. V. D., Forcade, R., & Jacobs, E. (1978). Circles of numbers. *Glasgow Math. J, 19,* 115-119.

Burmester, M. V. D., & Hughes, D. R. (1965). On the solvability of autotopism groups. *Archiv der Mathematik, Springer, 16(1),* 178-183.

Burmester, M. V. D. (1964). Sulla solubilità del gruppo delle collineazioni di un piano sopra un quasicorpo distributivo di ordine non-quadrata. *Accad. Nazionale dei Lincei, 36,* 1-4.

Burmester, M. V. D. (1964). On the non-uniqueness of translation planes over division rings. *Archiv der Matematik, Springer, 15,* 364-370.

Burmester, M. V. D. (1962). On the commutative non-associative division algebras of even order of L. E. Dickson. *Rend. Mat. e Appl, V. Ser. (6),* 143-166.

Invited Books

Burmester, M., Gritzalis, S., Katsikas, S., & Chrissikopoulos, V. (2011). *Modern Cryptography: Theory and Applications (pp. 728)*. Athens, Greece, Papasotiriou Pubs (in Greek).

Edited Books

García, C. R., Caballero-Gil, P., Burmester, M., & Quesada-Arencibia, A. (Eds.). (2016). *Ubiquitous Computing and Ambient Intelligence - 10th International Conference, UCAmI 2016, Proceedings Part II*. San Bartolomé de Tirajana, Gran Canaria, Spain, Lecture Notes in Computer Science 10070, Springer, Switzerland.

García, C. R., Caballero-Gil, P., Burmester, M., & Quesada-Arencibia, A. (Eds.). (2016). *Ubiquitous Computing and Ambient Intelligence - 10th International Conference, UCAmI 2016, Proceedings Part I*. San Bartolomé de Tirajana, Gran Canaria, Spain, Lecture Notes in Computer Science 10069, Springer, Switzerland.

Burmester, M., Tsudik, G., Magliveras, S. S., & Ilic, I. (Eds.). (2011). *Information Security - 13th International Conference (ISC 2010), Revised Selected Papers, Boca Raton, FL, USA*. Lecture Notes in Computer Science #6531, Springer-Verlag, Berlin.

Burmester, M., & Yasinsac, A. (Eds.). (2006). *International Workshop, Secure Mobile AD-hoc NEtworks and Sensors (MADNES'05), Revised Selected Papers*. Lecture Notes in Computer Science #4074, Springer-Verlag, Berlin.

Invited Book Chapters

Burmester, M. (2012). Localization Privacy. In David Naccache (Ed.), *Cryptography and Security: From Theory to Applications - Essays - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday* (pp. 425--441). Lecture Notes in Computer Science #6805, Springer-Verlag, Berlin.

Magkos, E., Burmester, M., & Chrissikopoulos, V. (2011). Ch. 14 Authenticated Key Establishment. In M. Burmester, S. Gritzalis, S. Katsikas, & V. Chrisikopoulos (Eds.), *Modern Cryptography: Theory and Applications* (pp. 499-538). Athens, Greece, Papasotiriou (in Greek).

Refereed Book Chapters

Redwood, W. O., Reynolds, J., & Burmester, M. (2016). Integrating Simulated Physics and Device Virtualization in Control System Tetbeds. In Sujeet Shenoi (Ed.), *Critical Infrastructure Protection X* (pp. pp 185-202). Springer, New York.

Jenkins, J., & Burmester, M. (2015). Run-Time Integrity for Cyber-Physical Infrastructures. In Mason Rice, & Sujeet Shenoi (Eds.), *Critical Infrastructure Protection IX, 9th IFIP WG 11.10* (pp. pp.153-167). Springer.

Redwood, O., & Burmester, M. (2015). A Symbolic Honeynet Framework for SCADA Threat Intelligence. In Mason Rice, & Shenoi Sujeet (Eds.), *Critical Infrastructure Protection IX, 9th IFIP WG 11.10* (pp. 103-118). Springer.

Jenkins, J., & Burmester, M. (2013). Chapter 6, Protecting infrastructure assets from real-time and run-time threats. In Butts, Jonathan, & Shenoi, Sujeet (Eds.), *Critical Infrastructure Protection VII* (pp. 97-110). Springer.

Burmester, M., & Redwood, O. W. (2013). Dynamic Trust Management: Network Profiling for High Assurance Resilience. In Evangelos Kranakis (Ed.), *Mathematics in Industry, Advances in Network Analysis and its Applications* (pp. 91-116). Springer-Verlag, Berlin. Retrieved from http://www.springer.com/new+%26+forthcoming+titles+%28default%29/book/978-3-642-30903-8

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2012). Modeling Security in Cyber-Physical Systems. In Shenoi, Sujeet (Ed.), *Critical Infrastructure Protection VI, IFIP WG 11.10* (pp. 118-126). Springer.

Burmester, M., & Munilla, J. (2012). RFID Grouping-Proofs. In Pedro Peris-Lopez, Julio C. Hernandez-Castro, & Tieyan Li. (Eds.), *Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID* (pp. 89-119). IGI Global.

Burmester, M. (2009). Trust Models for Ubiquitous Mobile Systems. In Humphry Hung, Y H Wong, & Vincent Cho (Eds.), *Ubiquitous Commerce for Creating the Personalized Marketplace: Concepts for Next Generation Adoption* (pp. 249-254). Idea Group Inc, Hershey, PA.

Hu, J., & Burmester, M. (2009). Cooperation in Mobile Ad Hoc Networks. In Sudip Misra, Isaac Wounsang, & Subhas Misra (Eds.), *Guide to Wireless Ad Hoc Networks* (pp. 43-58). London, Springer-Verlag.

Burmester, M. (2008). Section 1: Network Security and Survivability. In Evangelos Kranakis, Evgueni A. Haroutunian, & Elisa Shahbazia (Eds.), *Section 1. Aspects of Network and Information Security, NATO Science for Peace and Security Series: Information and Communication Security* (pp. 3-9). IOS Press.

De Medeiros, B., & Burmester, M. (2008). Ch 35. RFID Authentication: Reconciling Anonymity and Availability. In S. A. Ahson, & M. Ilyas (Eds.), *RFID Handbook: Application, Technology, Security, and Privacy* (pp. 642-655). CRC Press, Boca Raton, Fl.

Burmester, M., Kotzanikolaou, P., & Douligeris, C. (2007). Ch 20. Security in Mobile ad hoc networks. In Christos Douligeris, & Dimitris Serpanos (Eds.), *Network Security: Current status and future directions* (pp. 355-370). John Wiley & Sons.

Burmester, M., & Magkos, E. (2003). Towards Secure and Practical E-Elections in the New Era. In Dimitris Gritzalis (Ed.), *Secure Electronic Voting, Advances in Information Security* (pp. 63-76). Springer-Verlag, Berlin.

Burmester, M., Henderson, M., Dawson, E., & Okamoto, E. (2001). The Dark Side of Digital Signatures. In *Business Briefing - GLOBAL INFOSECURITY* (pp. 22). Information Technology Association of America (ITAA) and World Information Technology Service Alliance (WITSA).

Burmester, M., Desmedt, Y., & Kabatianski, G. (1997). A New Look at the Byzantine Generals Problem. In R.R. Wright, & P. Neuman (Eds.), *Network Threats, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Series 38* (pp. 75-83). American Mathematical Society.

Alexandris, N., Burmester, M., & Chrissikopouls, V. (1995). Cryptology for the Protection of Information. In N. Alexandris, E. Kiountouzis, & A. Trapezoglou (Eds.), *Information Security* (pp. 231-248). The Hellenic Society for Computers and Informatics, Athens, Greece.

Invited Monograph Chapters

Burmester, M. (2006). Trust and Confidence in a Wireless, Mobile Environment. In *eBusiness Forum Working Group ST3* (pp. 6). eBusiness Forum Working Group ST3.

Burmester, M., & Kotzanikolaou, P. (2006). Securing Networks Against Extreme Attacks. In *Essays in honor of Professor Antonios C. Panaiotopoulos* (pp. 875-886). University of Piraeus, Greece.

Refereed Encyclopedia Entries

Burmester, M. (2011). Group Key Agreement. In Henk C. A. van Tilborg and, & Sushil Jajodia (Eds.), *Encyclopedia of Cryptography and Security* (2nd ed., p. 520-526). Springer-Verlag, Berlin.

Burmester, M. (2005). Group Key Exchange. In Henk C.A.van Tilborg (Ed.), *Encyclopedia of Cryptography and Security* (1st ed.). Springer-Verlag, Berlin.

Refereed Proceedings

Burmester, M., Munilla, J., & Liu, X. (2017). Protecting the Supply Chain with RFID Technologies. In T. Morris (Ed.), Proceedings, *2017 National Cyber Summit (NCS 2017)* (pp. 79-84). Huntsville, AL.

Redwood, W. O., Burmester, M., & Liu, X. (2017). Offensive Computer Security Open Courseware. In T. Morris (Ed.), *Proceedings, 2017 National Cyber Summit (NCS 2017)* (pp. 69-72). Huntsville, AL.

Burmester, M., & Munilla Fajardo, J. (2016). Resilient Grouping Proofs with Missing Tag Identification. In Pino Caballero-Gil, Mike Burmester, & Carmelo R. Carcva (Eds.), *10th International Conference on Computing and Ambient Intelligence (UCAmI 2016), San Bartolomé de Tirajana, Gran Canaria, Spain* (pp. 544-555). Lecture Notes in Computer Science 10070, Springer.

Munilla Fajardo, J., & Burmester, M. (2016). Some Unsolved Concerns and Future Directions for Resilient RFID Smart Structures in the Supply Chain. In K. Wang (Ed.), *International Workshop on Advanced Manufacturing and Automation IWAMA 2016* (pp. 98-102). Manchester, U.K.: Advances in Economics, Business and Management Research, Atlantis Press.

Liu, X., Gibbens, A., Yang, J., Redwood, O., & Burmester, M. (2016). Offensive Computer Security Fundamentals Visualized via SecKoloring. In Morris, T (Ed.), *National Cyber Summit (NCS '16)* (pp. 6). Huntsville, AL.

Burmester, M., & Munilla, J. (2016). An Anonymous RFID Grouping-Proof with Missing Tag Identification. In *10th Annual IEEE International Conference on RFID (IEEE RFID 2016)* (pp. 146-152). Orlando, Florida, IEEE.

Burmester, M., & Munilla, J. (2016). Resilient Metro-Scale Smart Structures: Challenges & Future Directions. In Victor Chang, Muthu Ramachandran, Gary Wills, & Robert Walters (Eds.), *International Conference on Internet of Things and Big Data (IoTBD 2016)* (pp. 12). Rome, Italy.

Ho, S., Hancock, J., Booth, C., Burmester, M., Liu, X., & Timmarajus, S. (2016). Demystifying Insider Threat: Language-Action Cues in Group Dynamics. In *49th Hawaii International Conference on System Sciences* (pp. 2729--2738). Kauai, Hawaii.

Ho, S., Hancock, J., Booth, C., Liu, X., Liu, M., Timmarajus, S., & Burmester, M. (2016). Real or Spiel? A Decision Tree Approach for Automated Detection of Deceptive Language-Action Cues. In *49th Hawaii International Conference on System Sciences (HICSS)* (pp. 3706-3715). Kauai, Hawaii.

Ho, S. M., Hancock, J. T., Booth, C., Liu, X., Timmarajus, S., & Burmester, M. (2015). Liar, Liar, IM on Fire: Deceptive Language action Cues in Spontaneous Online Communication. In *IEEE Intelligence and Security Informatics (ISI 2015)* (pp. pp. 157-159). Baltimore, Maryland, IEEE.

Burmester, M., & Munilla, J. (2014). Group-scanning for Supply Chain Management. In Manos Tentzeris, & Apostolos Georgiadis (Eds.), *IEEE RFID Technology and Applications (RFID-TA)* (pp. 6). IEEE Xplore®.

Hu, J., & Burmester, M. (2014). Establishing a PKI in an Open Adversarial Environment. In *9th IEEE International Conference on Networking, Architecture, and Storage (NAS)* (pp. pp. 73-77). Tianjin, China.

Ho, S. M., Timmarajus, S. S., Burmester, M., & Liux, X. (2013). Dyadic attribution: A theoretical model for interpreting online words and actions. In *2014 International Conference on Social Computing, Behavioral-Cultural Modeling, & Prediction (SBP14)* (pp. 277-284). Springer, Lecture Notes in Computer Science (LCNS).

Jenkins, J., Easton, S., Guidry, D., Burmester, M., Liu, X., Yuan, S., Laurence, J., & Ty, S. (2013). Trusted Group Key Management For Real-Time Critical Infrastructure Protection. In *32nd annual Military Communications Conference, MILCOM 2013* (pp. 6). IEEE Communication Society.

Burmester, M. (2013). A Trusted Computing Architecture for Critical Infrastructure Protection. In Nikolaos Bourbakis, George A. Tsihrintzis, Maria Virvou, & Despina Kavraki (Eds.), *Fourth International Conference on Information, Intelligence, Systems and Applications (IISA 2013)* (pp. 1-6). Piraeus - Athens, IEEE Xplore.

Burmester, M., Magkos, E., & Chrissikopulos, V. (2013). T-ABAC: An Attribute-Based Access Control Model for Real-Time Availability in Highly Dynamic Systems. In Ivina Brandic, Stipe Celar, Hrvoje Dujmic, & Tajana Simunic Rosing (Eds.), *Eighth IEEE Symposium on Computers and Communications (ISCC'13)* (pp. 6). Split, Croatia, IEEE.

Burmester, M. (2013). Trusted Computing. In James Clark, Rebecca Wright, Julie Grady, Aljosa Pasic, Siani R Pearson, & Keyun Ruan (Eds.), *DIMAC/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC)* (pp. 6). Malaga, Spain, DIMACS.

Burmester, M., Laurence, J., Guidry, D., Easton, S., Ty, S., Liu, X., Yan, X., & Jenkins, J. (2013). Towards a Secure Electricity Grid. In *IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)* (pp. 6). Melbourne, Australia.

Jenkins, J., & Burmester, M. (2013). Trusted Computing for Critical Infrastructure Protection Against Real-time and Run-time Threats. In Jonathan Butts, & Sujeet Shenoi (Eds.), *Seventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection* (pp. 12). Washington, DC, IFIP.

Guidry, D., Burmester, M., Yuan, X., Liu, X., Jenkins, J., & Easton, S. (2012). Techniques for Securing Substation Automation Systems. In *Proceedings, 7th International Workshop on Critical Information Infrastructures Security (CRITIS 2012)* (pp. 10). Lillehammer, Norway.

Burmester, M. (2011). His Late Master's Voice: Barking for Location Privacy. In Bruce Christianson, Bruno Crispo, James A. Malcolm, & Frank Stajano (Eds.), *Security Protocols, XIX - 19th International Workshop, Cambridge, UK, March 28-30, 2011, Revised Selected Papers* (pp. 15-24). Lecture Notes in Computer Science (LNCS) Vol. 7114, Springer-Verlag, Berlin.

Burmester, M. (2010). Lightweight cryptographic mechanisms based on pseudorandom number generators. In Magliveras, Spyros (Ed.), *Lightweight cryptographic mechanisms Fourth Pythagorean Conference, Geometry, Combinatorial Designs and Cryptology*. Florida Atlantic University, Boca Raton.

Redwood, O., & Burmester, M. (2010). Markov anomaly modeling for Trust Management in variable threat environments. In Ruth, Paul, & Kraft, Nicholas A. (Eds.), *Proceedings of the 48th Annual ACM Southeast Regional Conference, Oxford, MS*. Art 114, ACM, New York.

Burmester, M., & Munilla, J. (2009). Flyweight authentication with forward and backward security. In *Flyweight authenWISP Summit 2009, First workshop on Wirelessly Powered Sensor Networks and Computational RFID* (pp. 1). Berkeley, California, INTEL.

Burmester, M., Das, P., Edwards, M., & Yasinsac, A. (2009). Multi-Domain trust management in variable threat environments —a user-centric model. In *Proceedings of the Military Communications Conference, 2009 (MILCOM 2009), Boston*. IEEE.

Burmester, M., De Medeiros, B., Munilla, J., & Peinado, A. (2009). Secure EPC Gen2 Compliant Radio Frequency Identification. In Pedro M. Ruiz, Jose Joaquin, & Garcia-Luna-Aceves (Eds.), *8th International Conference, Ad-Hoc Mobile and Wireless Networks (ADHOC-NOW 2009), Murcia, Spain* (pp. 227-240). Lecture Notes in Computer Science, Vol. 5793, Springer-Verlag, Berlin.

Burmester, M., & Munilla, J. (2009). A Flyweight RFID Authentication Protocol. In *Workshop on RFID Security 2009*. ESAT/SCD-COSIC, KU Leuven, Belgium.

Burmester, M., Safavi-Naini, R., & Taban, G. (2009). Secure Random Key Pre-Distribution Against Semi-Honest Adversaries. In *Sixth International Conference on Networked Sensing Systems (INSS09)*. Carnegie Mellon University, Pittsburgh.

Burmester, M., Das, P., Edwards, M., & Yasinsac, A. (2008). Multi-Domain trust management in variable threat environments using rollback-access. In *IEEE Proceedings of the Military Communications Conference, 2008 (MILCOM 2008), San Diego*. IEEE.

Burmester, M., Magkos, E., & Chrissikopoulos, V. (2008). Strengthening Privacy Protection in VANETs. In *IEEE International Conference on Wireless and Mobile Computing (WIMOB'08), Networking and Communications* (pp. 508-513). Avignon, France, IEEE.

Burmester, M., de Medeiros, B., & Motta, R. (2008). Provably secure grouping-proofs for RFID tags. In *8th International Conference on Smart Card Research and Advanced Applications (CARDIS 2008)* (pp. 176-190). Royal Holloway, Egham, Surrey, England, Lecture Notes in Computer Science #5185, Springer-Verlag, Berlin.

Batttacharia, B., Burmester, M., Hu, Y., Kranakis, E., Shi, Q., & Wiese, A. (2008). Optimal Movement of Mobile Sensors for Barrier Coverage of a Planar Region. In *2nd Annual International Conference on*

Combinatorial Optimization and Applications (COCOA'08) (pp. 103-115). St. Johns, Newfoundland, Canada, Lecture Notes in Computer Science #5165, Springer-Verlag, Berlin.

Burmester, M., & De Medeiros, B. (2008). The security of EPC Gen2 compliant RFID protocols. In *Proceedings, 6th International Conference on Applied Cryptography and Network Security (ACNS 2008), Columbia University, New York* (pp. 490-506). Lecture Notes in Computer Science, Vol. 5037, Springer-Verlag, Berlin.

Burmester, M., De Medeiros, B., & Motta, R. (2008). Robust, Anonymous RFID Authentication with Constant Key-Lookup. In Masayuki Abe, & Virgil D. Gligor (Eds.), *ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS 2008)*. Tokyo, Japan, ACM.

Tsudik, G., Burmester, M., Juels, A., Kobsa, A., Molnar, D., di Pietro, R., & Rieback, M. (2008). RFID security and privacy: long-term research or short-term tinkering? In *First ACM Conference on Wireless Network Security (WISEC 2008), Alexandria, VA* (pp. p. 160). ACM, New York, NY, USA. Retrieved from http://dl.acm.org/citation.cfm?id=1352560

Burmester, M., De Medeiros, B., & Motta, R. (2007). Anonymous RFID Authentication with Constant Lookup. In *6th RFID Academic Convocation, The RFID Journal Conference, Chicago* (pp. 5). The RFID Journal.

Burmester, M., & De Medeiros, B. (2007). Persistent Security for RFID. In *International Conference on RFID Security (RFIDSec07), Malaga, Spain* (pp. 101-112). University of Malaga. Retrieved from http://www.rfidsec07.etsit.uma.es/program/program.htm

Burmester, M., & De Medeiros, B. (2007). RFID Security: Attacks, Countermeasures and Challenges. In *5th RFID Academic Convocation, The RFID Journal Conference, Orlando* (pp. 9). The RFID Journal. Retrieved from http://www.rfidjournal.net/industry_newsletters/retail_030807.html

Burmester, M., De Medeiros, B., & Yasinsac, A. (2007). Community-centric vanilla-rollback access, or: How I stopped worrying and learned to love my computer. In *13th International Security Protocols Workshop, Cambridge, England* (pp. 228-237). Revised Selected Papers, Lecture Notes in Computer Science Vol. 4631, Springer-Verlag, Berlin.

Van Le, T., Burmester, M., & De Medeiros, B. (2007). Universally Composable and Forward-secure RFID Authentication and Authenticated Key Exchange. In *ACM Symposium on InformAtion, Computer and Communications Security (ASIACCS'07) Singapore* (pp. 242-252). ACM New York, USA.

Desmedt, Y., Lang, T., & Burmester, M. (2007). Scalable Authenticated Tree Based Group Key Exchange for Ad-Hoc Groups. In *11th International Conference, Financial Cryptography and Data Security (FC'07), Trinidad* (pp. 104-118). Lecture Notes in Computer Science #4886, Springer-Verlag, Berlin.

Burmester, M., de Medeiros, B., & vam Le, T. (2006). Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. In *2nd International Conference on Security and Privacy in Communication Networks (SecureComm 2006), Baltimore* (pp. 1-9). IEEE.

Burmester, M., Gligor, V., Kranakis, E., Tyger, D., & Zheng, Y. (2006). Authentication in constrained Environments. In Mike Burmester, & Alec Yasinsac (Eds.), *Secure Mobile Ad-hoc networks and Sensors (MADNES 2005), Singapore* (pp. 186-191). Lecture Notes in Computer Science # 4078, Springer-Verlag, Berlin.

Desmedt, Y., Wang, Y., & Burmester, M. (2006). Revisiting Colored Networks and Privacy Preserving Censorship. In *1st International Workshop on Critical Information Infrastructure Security, CRITIS 2006* (pp. 140-150). Lecture Notes in Computer Science #4347, Springer-Verlag, Berlin.

Burmester, M., van Le, T., & de Medeiros, B. (2006). Towards Provable Security for Ubiquitous Applications. In *11th Australasian Conference, Information Security and Privacy (ACISP 2006)* (pp. 295-312). Lecture Notes in Computer Science #4058, Springer-Verlag, Berlin.

Burmester, M., Desmedt, Y., Wright, R., & Yasinsac, A. (2006). Accountable Privacy. In *12th International Security Protocols Workshop, Cambridge, England* (pp. 83-95). Lecture Notes in Computer Science #3957, Springer-Verlag, Berlin.

Burmester, M., & Mulholland, J. (2006). The Advent of Trusted Computing: Implications for Digital Forensics. In Hisham Haddad (Ed.), *21st ACM Symposium on Applied Computing, Computer Forensics Track (SAC 2006), Dijon, France* (pp. 283-287). ACM.

Burmester, M., & Hu, J. (2006). LARS - A Locally Aware Reputation System for Mobile Ad hoc Networks, Melbourne, Florida. In *44th ACM Southeast Regional Conference* (pp. 119-123). ACM New York.

Burmester, M., & Van Le, T. (2006). Optimistic fault tracing and adaptive multipath routing in MANETs. In *NSF Int. Workshop on Research Challenges in Security and Privacy for Mobile Wireless Networks (WSPWN'06)* (pp. 45-60). Miami.

Burmester, M., & Van Le, T. (2006). Reactive and Proactive Approaches to Secure Routing in MANETs. In *NSF Int. Workshop on Research Challenges in Security and Privacy for Mobile Wireless Networks (WSPWN'06)* (pp. 10). Miami.

Desmedt, Y., Wang, Y., & Burmester, M. (2005). A Complete Characterization of Tolerable Adversary Structures for Secure Point-to-Point Transmissions. In *16th International Symposium on Algorithms and Computation (ISAAC 2005), Hainan, China* (pp. 277-287). Lecture Notes in Computer Science #3827, Springer-Verlag, Berlin.

Aggarwal, S., Burmester, M., Henry, P., Kermes, L., & Mulholland, J. (2005). Anti Cyberstalking: The Predator and Prey Alert (PAPA) System. In *First International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE '05)* (pp. 195-205). IEEE Computer Society, Washington, DC, USA.

Burmester, M. (2005). Information Theory, Cryptography and the Internet (in Greek). In *22nd Panhellenic Conference on Mathematical Education, Lamia, Greece* (pp. 744-754). The Hellenic Mathematical Society.

Burmester, M., & Yasinsac, A. (2005). Protocols for Supporting a Public Key Infrastructure in Ad Hoc Networks. In *11th International Workshop on Security Protocols, Cambridge, England, April 2–4, 2002*. Lecture Notes in Computer Science #336, Springer-Verlag, Berlin.

Desmedt, Y., & Burmester, M. (2004). Identity-based Key Infrastructures (IKI). In Yves Deswarte, Frédéric Cuppens, Sushil Jajodia, Lingyu Wang, & 147, pp. 167 - 176, 2004 (Eds.), *Security and Protection in Information Processing Systems, IFIP 18th WorldComputer Congress, TC11 19th International Information Security Conference, Toulouse, France* (pp. 167-176). Kluwer.

Burmester, M., Van Le, T., & Yasinsac, A. (2004). Weathering the Storm: Managing Redundancy and Security in Ad Hoc Networks. In Ioanis Nikolaidis, Michel Barbeau, & Evangelos Kranakis (Eds.), *Ad-Hoc, Mobile, and Wireless Networks: Third International Conference, ADHOC-NOW 2004, Vancouver, Canada* (pp. 96-107). Lecture Notes in Computer Science #3158, Springer-Verlag, Berlin.

Burmester, M., & Van Le, T. (2004). Secure Communication in Ad hoc Networks. In *5th Annual IEEE Information Assurance Workshop (IAW 2004), West Point, New York* (pp. 234-241). IEEE Conference Publications.

Burmester, M., & Van Le, T. (2004). Secure Multipath Communication in Mobile Ad hoc Networks. In *International Conference on Information Technology Coding and Computing (ITCC04), Las Vegas, Nevada* (pp. 405--409). IEEE Computer Society.

Burmester, M., & Desmedt, Y. (2003). A Critical Analysis of Models for Fault-Tolerant and Secure Computation. In M.H. Hamza (Ed.), *Communication, Network, and Information Security (CNIS 2003)* (pp. 147-152). ACTA Press.

Burmester, M., Van Le, T., & Weir, M. (2003). Tracing Byzantine faults in ad hoc networks. In M.H. Hamza (Ed.), *Communication, Network, and Information Security (CNIS 2003)* (pp. 105--106). ACTA Press.

Van Le, T., Burmester, M., & Hu, J. (2003). Short c-secure Fingerprinting Codes. In *6th Information Security Conference (ISC'03), Bristol, UK* (pp. 422-427). Lecture Notes in Computer Science Vol. 2851, Springer-Verlag, Berlin.

Yvo, D., Burmester, M., & Kurasawa, K. (2002). On Perfect Traitor Tracing. In *IEEE International Symposium on Information Theory, Lausanne, Switzerland* (pp. 439). IEEE.

Adams, C., Burmester, M., Desmedt, Y., Reiter, M., & Zimmermann, P. (2001). Panel: Which PKI (public key infrastructure) is the right one? In Sushil Jajodia, & Pierangela Samarati (Eds.), *7th ACM Conference on Computer and Communications Security, Athens, Greece* (pp. 98--01). ACM New York, NY, USA.

Burmester, M., & Desmedt, Y. (2001). Hierarchical public-key certification: the next target for hackers. In *1st International Workshop for Asian Public key Infrastructures (IWAP 2001), Daejon, Korea* (pp. 31-43). International Research Center for Information Security, Korea.

Burmester, M., Magkos, E., & Chrissikopouls, V. (2001). Receipt-Freeness in Large-Scale Elections without Untappable Channels. In B. Schmid, K. Stanoevska-Slabeva, & V. Tschammer (Eds.), *Towards The E-Society: E-Commerce, E-Business, and E-Government, The First IFIP Conference on E-Commerce, E-Business, E-Government (I3E 2001), Zürich, Switzerland* (pp. 683-694). IFIP Conference Proceedings, Kluwer.

Kotzanikilaou, P., Burmester, M., & Chrissikopoulos, V. (2001). Dynamic Multi-signatures for Secure Autonomous Agents. In A. Min Tjoa, & Roland Wagner (Eds.), *12th International Workshop on Database and Expert Systems Applications (DEXA 2001)* (pp. 587-591). IEEE Computer Society.

Burmester, M., Chrissikopoulos, V., Kotzanikolaou, P., & Magkos, E. (2001). Strong Forward Security. In M. Dupuy, & P. Paradinas (Eds.), *IFIP-TC11 Sixteenth Annual Conference on Information Security (IFIP/ SEC '01), Trusted Information – The New Decade Challenge, Vol. 193, Paris, France* (pp. 109-119). Kluwer Academic Publishers, Boston.

Desmedt, Y., Burmester, M., Safavi-Naini, R., & Wang, H. (2001). Threshold Things That Think (T4): Security Requirements to Cope with Theft of Handheld/Handless Internet Devices. In *Symposium on Requirements Engineering for Information Security (SREIS), Indianapolis* (pp. 354-367). Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University.

Desmedt, Y., Burmester, M., & Seberry, J. (2001). Equitability in Retroactive Data Confiscation versus Proactive Key Escrow. In Kwangjo Kim (Ed.), *4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), Cheju Island, Korea* (pp. 277-286). Lecture Notes in Computer Science Vol. 1992, Springer-Verlag, Berlin.

Henderson, M., Burmester, M., Ed Dawson, E., & Okamoto, E. (2000). Weaknesses in Public Key Infrastructures. In *Proc. 1st Workshop in Information Security Applications, Seoul, Korea* (pp. 53-66). Korea Institute of Information Security and Cryptology (KIISC).

Burmester, M., Desmedt, Y., Alexandris, N., & Chrissikopoulos, V. (2000). Designated 2-Verifier Proofs and their Application to Electronic Commerce. In Kwok-Yan Lam, Huaxiong Wang, Igor E Sparlinskij, & Chaoping Xing (Eds.), *Cryptography and computational number theory : Proceedings of the workshop on Cryptography and Computational Number Theory, CCNT'99, Singapore Nov 1999* (pp. 149-164). Basel : Birkhäuser Verlag.

Burmester, M., Desmedt, Y., Doi, H., Mambo, M., & Yosifuji, Y. (2000). A Structured ElGamal-Type Multisignature Scheme. In Hideki Imai, & Yuliang Zheng (Eds.), *Public Key Cryptography, Third International Workshop on Practice and Theory in Public Key Cryptography (PKC 2000), Melbourne, Australia* (pp. 466-483). Lecture Notes in Computer Science Vol. 1751, Springer-Verlag, Berlin.

Kotzanikolaou, P., Burmester, M., & Chrissikopoulos, V. (2000). Secure Transactions with Mobile Agents in Hostile Environments. In Ed Dawson, Andrew Clark, & Colin Boyd (Eds.), *5th Australasian Conference (ACISP 2000), Information Security and Privacy, Brisbane, Australia* (pp. 289-297). Lecture Notes in Computer Science, Vol. 1841, Springer-Verlag, Berlin.

Magkos, E., Burmester, M., & Chrissikopoulos, V. (2000). An Equitably Fair On-line Auction Scheme. In Kurt Bauknecht, Sanjay Kumar Madria, & Günther Pernul (Eds.), *Electronic Commerce and Web Technologies, First Int. Conf. EC-Web 2000, London, UK* (pp. 72-83). Lecture Notes in Computer Science Vol. 1875, Springer-Verlag, Berlin.

Burmester, M., Desmedt, Y., & Seberry, J. (1999). Equitable Key Escrow with Limited Time Span (or, How to Enforce Time Expiration Cryptographically. In Kazuo Ohta, & Dingyi Pei (Eds.), *Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China* (pp. 18-22). Lecture Notes in Computer Science Vol. 1514, Springer-Verlag, Berlin.

Kurosawa, K., Yoshida, T., Desmedt, Y., & Burmester, M. (1999). Some Bounds and a Construction for Secure Broadcast Encryption. In Kazuo Ohta, & Dingyi Pei (Eds.), *Advances in Cryptology - ASIACRYPT '98, International Conference on the Theory and Applications of Cryptology and Information Security, Beijing, China* (pp. 420-433). Lecture Notes in Computer Science Vol. 1514, Springer-Verlag, Berlin.

Blackburn, S., Blake-Wilson, S., Burmester, M., & Galbraith, S. (1999). Weaknesses in Shared RSA Key Generation Protocols. In Michael Walker (Ed.), *7th IMA International Conference, Cryptography and Coding, Cirencester, England* (pp. 7300-306). Lecture Notes in Computer Science Vol. 1746, Springer-Verlag, Berlin.

Burmester, M., & Desmedt, Y. (1999). Secure Communication in an Unknown Network Using Certificates. In Kwok-Yan Lam, Eiji Okamoto, & Chaoping Xing (Eds.), *Advances in Cryptology - Asiacrypt '99* (pp. 274–287). Lecture Notes in Computer Science Vol. 1716, Springer, Berlin-Verlag, Berlin.

Burmester, M., Desmedt, Y., & Wang, Y. (1998). Using Approximation Hardness to Achieve Dependable Computation. In Michael Luby, Josè D. P. Rolim, & Maria J. Serna (Eds.), *Randomization and Approximation Techniques in Computer Science, Second International Workshop, RANDOM'98, Barcelona, Spain* (pp. 172-186). Lecture Notes in Computer Science Vol. 1518, Springer-Verlag, Berlin.

Bassalygo, L. A., Burmester, M., Dyachkov, A., & Kabatianski, G. (1997). Hash Codes. In *IEEE International Symposium on Information Theory (ISIT'1997)* (pp. 174). IEEE.

Alexandris, N., Burmester, M., & Chrissikopoulos, V. (1997). Secure Group Communications: a dynamic approach. In S.K. Katsikas (Ed.), *Communications and Multimedia Security (CMS '97)* (pp. 41-51). Chapman & Hall.

Alexandris, N., Burmester, M., Chrissikopoulos, V., & Peppes, D. (1996). Efficient and provably secure key agreement. In Sokratis K. Katsikas, & Dimitris Gritzalis (Eds.), *Information Systems Security, Facing the information society of the 21st Century (SEC)* (pp. 227-236). IFIP Conference Proceedings Vol. 54, Chapman & Hall.

Burmester, M., Desmedt, Y., Ito, T., Sakurai, K., Shizuya, H., & Yung, M. (1996). A Progress Report on Subliminal-Free Channels. In Ross J. Anderson (Ed.), *Information Hiding, First International Workshop, Cambridge* (pp. 157-168). Lecture Notes in Computer Science Vol. 1174, Springer-Verlag, Berlin.

Blackburn, S. R., Burmester, M., Desmedt, Y., & Wild, Peter, R. (1996). Efficient Multiplicative Sharing Schemes. In Ueli M. Maurer (Ed.), *Advances in Cryptology - EUROCRYPT '96, Int. Conf. on the Theory and Application of Cryptographic Techniques, Saragossa, Spain* (pp. 107-118). Lecture Notes in Computer Science Vol. 1070, Springer-Verlag, Berlin.

Burmester, M. (1996). Homomorphisms of Secret Sharing Schemes: A Tool for Verifiable Signature Sharing. In Ueli M. Maurer (Ed.), *Advances in Cryptology - EUROCRYPT '96, Int. Conf. on the Theory and Application of Cryptographic Techniques, Saragossa, Spain* (pp. 96-106). Lecture Notes in Computer Science Vol. 1070, Springer-Verlag, Berlin.

Burmester, M., & Desmedt, Y. (1996). Efficient and Secure Conference-Key Distribution. In T. Mark A. Lomas (Ed.), *Security Protocols, International Workshop, Cambridge, United Kingdom* (pp. 119-129). Lecture Notes in Computer Science Vol. 1189, Springer, Berlin.

Desmedt, Y., Di Crescenzo, G., & Burmester, M. (1995). Multiplicative Non-abelian Sharing Schemes and their Application to Threshold Cryptography. In Josef Pieprzyk, & Reihaneh Safavi-Nain (Eds.), *Advances in Cryptology - ASIACRYPT '94, 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia* (pp. 21-32). Lecture Notes in Computer Science Vol. 917, Springer-Verlag, Berlin.

Burmester, M., & Desmedt, Y. (1995). A Secure and Efficient Conference Key Distribution System. In Alfredo De Santis (Ed.), *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy* (pp. 275-286). Lecture Notes in Computer Science Vol. 950, Springer-Verlag, Berlin.

Burmester, M., Alexandris, N., Chrissikopoulos, V., & Pepes, D. (1995). Key agreement protocols: two efficient models for provable security. In *5th Panhellenic Conference on Information Theory, Athens, Greece* (pp. 177-187). Hellenic Mathematical Society.

Burmester, M. (1994). On the Risk of Opening Distributed Keys. In Yvo Desmedt (Ed.), *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA* (pp. 308-317). Lecture Notes in Computer Science vol. 839, Springer-Verlag, Berlin.

Chen, L., & Burmester, M. (1994). A practical voting scheme which allows voters to abstain. In *Chinacrypt '94* (pp. 100-107). Xidian, China.

Burmester, M. (1994). Cryptoanalysis of the Chang-Wu-Chen Key Distribution System. In Tor Helleseth (Ed.), *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway* (pp. 440-442). Lecture Notes in Computer Science Vol. 765, Springer-Verlag, Berlin.

Desmedt, Y., & Burmester, M. (1993). Towards Practical ``Proven Secure'' Authenticated Key Distribution. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, & Victoria Ashby (Eds.), *CCS '93, Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA* (pp. 228-231). ACM.

Desmedt, Y., & Burmester, M. (1993). An Efficient Zero-Knowledge Scheme for the Discrete Logarithm Based on Smooth Numbers. In Hideki Imai, Ronald L. Rivest, & Tsutomu Matsumoto (Eds.), *Advances in*

Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Fujiyoshida, Japan (pp. 360-367). Lecture Notes in Computer Science Vol. 739, Springer-Verlag, Berlin.

Frankel, Y., Desmedt, Y., & Burmester, M. (1993). Non-Existence of Homomorphic General Sharing Schemes for Some Key Spaces. In Ernest F. Brickell (Ed.), *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA* (pp. 549-557). Lecture Notes in Computer Science Vol. 740, Springer-Verlag, Berlin.

Alexandris, N., Burmester, M., Chrissikopulos, V., & Desmedt, Y. (1993). A secure key distribution system. In W. Wolfowicz (Ed.), *3rd Symposium on: State and Progress of Research in Cryptography* (pp. 30-34). Fondazione Ugo Bordoni, Rome.

Burmester, M., Alexandris, N., & Chrissikopulos, V. (1993). Network security and authentication (in greek). In *4th Panhellenic Conference on Information Theory, Vol II, Patras* (pp. 249-256). Hellenic Mathematical Society (EPI).

Alexandris, N., Burmester, M., & Chrissikopoulos, V. (1992). An Efficient Public Key Distribution System. In Robert M. Aiken (Ed.), *Education and Society - Information Processing '92, Volume 2, Proceedings of the IFIP 12th World Computer Congress, Madrid, Spain* (pp. 532-539). IFIP Transactions A-13, North-Holland.

Burmester, M., & Desmedt, Y. (1992). Zero-Knowledge Based Identification: From a Theoretical Concept Towards a Practical Token. In Robert M. Aiken (Ed.), *Education and Society - Information Processing '92, Volume 2, Proceedings of the IFIP 12th World Computer Congress, Madrid, Spain* (pp. 479-485). IFIP Transactions A-13, North-Holland.

Desmedt, Y., & Burmester, M. (1992). An efficient zero-knowledge scheme for the discrete logarithm based on smooth numbers. In H. Imai, R.L. Rivest, & T. Matsumoto (Eds.), *Advances in Cryptology – Asiacrypt '91* (pp. 360-367). Lecture Notes in Computer Science #739, Springer-Verlag, Berlin.

Burmester, M., & Desmedt, Y. (1991). Broadcast Interactive Proofs. In D. W. Davies (Ed.), *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK* (pp. 81-95). Lecture Notes in Computer Science Vol. 547, Springer-Verlag, Berlin.

Burmester, M. (1991). A Remark on the Efficiency of Identification Scheme. In Ivan Damgard (Ed.), *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark* (pp. 493-495). Lecture Notes in Computer Science Vol. 473, Springer-Verlag, Berlin.

Burmester, M., & Desmedt, Y. (1991). All Languages in NP Have Divertible Zero-Knowledge Proofs and Arguments Under Cryptographic Assumptions. In I. Damgard (Ed.), *Advances in Cryptology - EUROCRYPT '90, Workshop on the Theory and Application of of Cryptographic Techniques, Aarhus, Denmark* (pp. 1-10). Lecture Notes in Computer Science Vol. 473, Springer-Verlag, Berlin.

Burmester, M., Chrissikopulos, V., & Alexandris, N. (1991). Applications of cryptography to network security. In *3rd Panhellenic Conference on Information Theory, Athens* (pp. 570-580). Hellenic Information Association (EPY).

Burmester, M., Desmedt, Y., & Yung, M. (1991). Subliminal-free channels: a solution towards covert-free channels. In W. Wolfowicz (Ed.), *Symposium on Computer Security, Threats and Countermeasures* (pp. 188-197). Fondazione Ugo Bordoni, Rome.

Burmester, M., Desmedt, Y., Piper, F., & Walker, M. (1990). A General Zero-Knowledge Scheme. In J.-J. Quisquater, & J. Vandewalle (Eds.), *Advances in Cryptology - Eurocrypt '89, Workshop on the Theory and Application of of Cryptographic Techniques, Houthalen, Belgium* (pp. 122-133). Lecture Notes in Computer Science Vol. 434, Springer-Verlag, Berlin.

Burmester, M. V. D. (1967). Automorphisms of division rings. In *Symposium on Projective Geometry* (pp. 13-15). University of Illinois, Chicago.

Presentations

Refereed Papers at Conferences

Burmester, M. (presented 2016, December). *Resilient Grouping Proofs with Missing Tag Identification*. Paper presented at 10th International Conference on Computing and Ambient Intelligence (UCAmI 2016), Ubiquitous Computing and Ambient Intelligence, San Bartolomé de Tirajana, Gran Canaria, Spain. (International)

Burmester, M. (presented 2016, June). *Offensive Computer Security Fundamentals Visualized via SecKoloring*. Paper presented at 2016 National Cyber Summit, National Cyber Summit, Huntsville, Alabama. (International)

Burmester, M. (presented 2016, May). *An Anonymous RFID Grouping-Proof with Missing Tag Identification*. Paper presented at 10th Annual IEEE International Conference on RFID (IEEE RFID 2016), IEEE, Orlando, Florida. (International)

Burmester, M. (presented 2016, April). *Resilient Metro-Scale Smart Structures: Challenges & Future Directions*. Paper presented at International Conference on Internet of Things and Big Data, Institute for Systems and Technologies of Information, Control and Communication (INSTICC), Rome, Italy. (International)

Burmester, M. (presented 2015, March). *Run-Time Integrity for Cyber-Physical Infrastructures*. Paper presented at Ninth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, IFIP WG 11.10, International Federation for Information Processing (IFIP WG 11.10), Arlington, Virginia, USA. (International)

Burmester, M. (presented 2013, July). *T-ABAC: An Attribute-Based Access Control Model for Real-Time Availability in Highly Dynamic Systems*. Paper presented at Eighth IEEE Symposium on Computers and Communications (ISCC'13), IEEE, Split, Croatia. (International)

Burmester, M. (presented 2013, April). *Towards a Secure Electricity Grid*. Paper presented at IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP 2013), IEEE, Melbourne, Australia. (International)

Burmester, M. (presented 2013, March). *Trusted Computing for Critical Infrastructure Protection Against Real-time and Run-time Threats*. Paper presented at Seventh Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, International Federation for Information Processing (IFIP WG 11.10), Washington, DC. (International)

Burmester, M. (presented 2012, September). *Techniques for Securing Substation Automation Systems*. Paper presented at Critical Information Infrastructures Security (CRITIS 2012), Lillehammer, Norway, Høgskolen i Gjøvik. (International)

Burmester, M. (presented 2011, March). *His Late Master's Voice: Barking for location privacy*. Paper presented at 19th International Workshop on Security Protocols, University of Cambridge, England. (International)

Burmester, M. (presented 2010, June). *Lightweight cryptographic mechanisms based on pseudorandom number generators*. Paper presented at Fourth Pythagorean Conference, Geometry, Combinatorial Designs and Cryptology, Corfu, Greece, Florida Atlantic University. (International)

Burmester, M. (presented 2010, June). *Network Profiling for High Assurance Survivability*. Paper presented at Workshop on Network Security & Cryptography, Toronto, MITACS, Canada. (International)

Burmester, M. (presented 2010, June). *Network Profiling for High Assurance Survivability*. Paper presented at Network Profiling for High Workshop on Network Security & Cryptography, Toronto, Canada, MITACS. (International)

Burmester, M. (presented 2008, November). *Multi-Domain trust management in variable threat environments using rollback-access*. Paper presented at The Military Communications Conference, 2008 (MILCOM-08), IEEE, San Diego, CA. (International)

Burmester, M. (presented 2008, September). *Provably Secure Grouping-Proofs for RFID Tags*. Paper presented at Provably Secure Grouping-Proofs for RFID Tags – 8th International Conference on Smart Card Research and Advanced Applications (CARDIS 2008), Royal Holloway, Egham, England. (International)

Burmester, M. (presented 2008, August). *Movement of Mobile Sensors for Barrier Coverage of a Planar Region*. Paper presented at 2nd Annual International Conference on Combinatorial Optimization and Applications (COCOA 2008), St. Johns, Memorial University of Newfoundland, Canada. (International)

Burmester, M. (presented 2008, April). *RFID security and privacy: long-term research or short-term tinkering?* Paper presented at 1st ACM Conference on Wireless Network Security (WISEC 2008), Alexandria, VA, USA, ACM. (International)

Burmester, M. (presented 2007, October). *Anonymous RFID Authentication with Constant Key-Lookup*. Paper presented at 6th RFID Academic Convocation, The RFID Journal. (National)

Burmester, M. (presented 2007, July). *Persistent Security for RFID*. Paper presented at RFID Security (RFIDSec07), University of Malaga, Spain. (National)

Burmester, M. (presented 2007, May). *RFID Security: Attacks, Countermeasures and Challenges*. Paper presented at 5th RFID Academic Convocation, Orlando, The RFID Journal. (International)

Burmester, M. (presented 2007, March). *Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange*. Paper presented at ACM Symposium on Information, Computer and Communications Security (ASIACCS'07), Singapore, ACM. (International)

Burmester, M. (presented 2006, March). *Reactive and Proactive approaches to Secure Routing in MANETs*. Paper presented at NSF International Workshop on Research Challenges in Security and Privacy for Mobile Wireless Networks, Miami, NSF. (National)

Burmester, M. (presented 2005, April). *Community-centric vanilla-rollback access, or: How I stopped worrying and learned to love my computer*. Paper presented at Thirteenth International Workshop on Security Protocols, Cambridge, University of Hertfordshire, England. (International)

Burmester, M. (presented 2004, July). *Weathering the storm: managing redundancy and security in ad hoc networks*. Paper presented at Third International Conference on Ad hoc and Wireless networks, ADHOC-NOW'04, Vancouver, University of British Columbia. (National)

Burmester, M. (presented 2004, April). *Responsible Privacy*. Paper presented at 12th International Workshop on Security Protocols, Cambridge, University of Hertfordshire, England. (International)

Burmester, M. (presented 2004, April). *Secure Multipath Communication in Mobile Ad hoc Networks*. Paper presented at International Conference on Information Technology Coding and Computing (ITCC 2004), Las Vegas, Nevada, IEEE Computer Society. (International)

Burmester, M. (presented 2003, December). *A Critical Analysis of Models for Fault-Tolerant and Secure Computation*. Paper presented at IASTED International Conference on Computer, Network and Information Security (CNIS 2003), International Association of Science and Technology for Development, New York. (International)

Burmester, M. (presented 2003, December). *Tracing Byzantine faults in ad hoc networks*. Paper presented at IASTED International Conference on Computer, Network and Information Security (CNIS 2003), International Association of Science and Technology for Development, New York. (International)

Burmester, M. (presented 2003, October). *Short c-secure Fingerprinting Codes.* Paper presented at 6th Information Security Conference (ISC'03), Hewlett-Packard Laboratories, Bristol, United Kingdom. (International)

Burmester, M. (presented 2001, June). *Strong Forward Security*. Paper presented at 16th International Conference on Information Security, IFIP/TC11, Paris, France. (International)

Burmester, M. (presented 2000, July). *Secure Transactions with Mobile Agents in Hostile environments*. Paper presented at 5th Annual Australasian Conference on Information Security and Privacy (ACISP 2000), Queensland University of Technology, Brisbane, Australia. (International)

Burmester, M. (presented 2000, July). *Securing Large E-Commerce Networks.* Paper presented at 5th Annual Australasian Conference on Information Security and Privacy (ACISP 2000), Queensland University of Technology, Brisbane, Australia. (International)

Burmester, M. (presented 1999, November). *Secure Communication in an Unknown Network Using Certificates*. Paper presented at International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 99), International Association for Cryptology Research, Singapore. (International)

Burmester, M. (presented 1999, September). *Secure Group Communications: a dynamic approach*. Paper presented at IFIP Joint Working Conference, Communications and Multimedia Security (CMS '97), IFIP TC6/TC11, Athens, Greece. (International)

Burmester, M. (presented 1996, December). *A network security threat in general, even when cryptography is used*. Paper presented at DIMACS Workshop on Network Threats, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Newark NY. (National)

Burmester, M. (presented 1996, October). *Linking trust with network reliability*. Paper presented at DIMACS Workshop on Network Threats, Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), Newark NY. (National)

Burmester, M. (presented 1996, October). *New directions in Mathematics: the management and protection of information*. Paper presented at Mathematics in Education and Society, Panhellenic Congress, Hellenic Mathematical Society, Athens, Greece. (National)

Burmester, M. (presented 1996, May). *Efficient and provably secure key agreement*. Paper presented at Information Systems Security, Facing the Information Society of the 21st century (IFIP SEC '96), International Federation for Information Processing, Samos, Greece. (International)

Burmester, M. (presented 1996, May). *Efficient Multiplicative Sharing Schemes*. Paper presented at EUROCRYPT '96, International Association for Cryptologic Research, Zaragoza, Spain. (International)

Burmester, M. (presented 1996, May). *Homomorphisms of Secret Sharing Schemes: a Tool for Verifiable Signature Sharing*. Paper presented at EUROCRYPT '96, International Association for Cryptologic Research, Zaragoza, Spain. (International)

Burmester, M. (presented 1995, December). *Key agreement protocols: two efficient models for provable security*. Paper presented at 5th Panhellenic Conference on Information Theory, Hellenic Society for Computers and Informatics, Athens, Greece. (National)

Burmester, M. (presented 1994, August). *On the risk of opening distributed keys*. Paper presented at Crypto '94, International Association for Cryptologic Research, Santa Barbara, CA, USA. (International)

Burmester, M. (presented 1994, May). *A secure and efficient conference key distribution system*. Paper presented at Eurocrypt '96, International Association for Cryptologic Research, Perugia, Italy. (International)

Burmester, M. (presented 1993, November). *Towards practical 'proven secure' authenticated key distribution –*. Paper presented at 1st ACM Conference on Computer and Communications Security, ACM, Fairfax, Virginia. (International)

Burmester, M. (presented 1993, May). *Cryptanalysis of the Chang-Wu-Chen key distribution system*. Paper presented at Eurocrypt '93, International Association for Cryptologic Research, Lofthus, Norway. (International)

Burmester, M. (presented 1993, February). *A secure key distribution system*. Paper presented at 3rd Symposium on State and Progress of Research in Cryptography (SPRC '93), Fondazione Ugo Bordoni, Rome, Italy. (International)

Burmester, M. (presented 1992, September). *An efficient public key distribution system*. Paper presented at IFIP 12th World Computer Congress, International Federation for Information Processing, Madrid, Spain. (International)

Burmester, M. (presented 1992, September). *Zero-knowledge Based Identification: From a Theoretical Concept Towards a Practical Token*. Paper presented at IFIP 12th World Computer Congress, International Federation for Information Processing, Madrid, Spain. (International)

Burmester, M. (presented 1992, August). *Non-existence of homomorphic general sharing schemes for some key spaces*. Paper presented at Crypto '92, International Association for Cryptologic Research, Santa Barbara, CA. (International)

Invited Keynote and Plenary Presentations at Conferences

Burmester, M. (presented 2015, December). *Reliability & resilience for emergencies and critical infrastructure*. Keynote presentation at 1st Workshop for Mobile Tools for Emergencies & Critical Infrastructures, University of La Laguna, Tenerife, Spain. (International) Retrieved from http://cryptull.webs.ull.es/CASUS/WEBCASUScontenido/workshop1/index.htm

Burmester, M. (presented 2014, April). *Reliable and resilient interdependent systems*. Keynote presentation at II Workshop on Security in Internet of Things (SIT), University of La Laguna, Tenerife Spain. (International)

Burmester, M. (presented 2013, July). *Trusted Computing for Critical infrastructures*. Keynote presentation at Fourth International Conference on Information, Intelligence, Systems and Applications IISA 2013, IEEE, University of Piraeus, Piraeus, Greece. (International)

Burmester, M. (presented 2013, March). *Localization privacy for RFID*. Keynote presentation at SIT2013, Workshop on Security in Internet of Things, University of La Laguna, Tenerife, SPAIN. (International)

Burmester, M. (presented 2007, March). *Resilient Ad-hoc Networking Supporting Fault Traceability*. Keynote presentation at Communication, Networks and Security (CNS), Carlton Wireless Security Day, Ottawa, MITACS, Canada. (International)

Burmester, M. (presented 2007, March). *Secure Group Key Exchange, Revisited I & II –*. Keynote presentation at 38th Southeastern International Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Florida. (International)

Burmester, M. (presented 2006, July). *Towards provable security for ubiquitous applications*. Keynote presentation at 11th Annual Australasian Conference on Information Security and Privacy ACISP, Melbourne, International Association of Cryptological Research, Australia. (International)

Burmester, M. (presented 2006, March). *Provable Security for MANETs*. Keynote presentation at NSF International Workshop on Research in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006), NSF, Miami. (International)

Burmester, M. (presented 2005, November). *Theory of Information, Cryptograsphy and the Internet*. Keynote presentation at Panhellenic Conference on Mathematical Education, The Hellenic Mathematical Society, Lamia, Greece. (National)

Burmester, M. (presented 2005, June). *Extreme Security – Network-centric Information Systems*. Keynote presentation at One-day Workshop, University of Piraeus, Greece. (National)

Burmester, M. (presented 2003, October). *Securing Ad hoc Networks*. Keynote presentation at 3rd Annual Conference on Information Security: From Theory to Practice, Nicosia, Cyprus Computer Society, Cyprus. (National)

Burmester, M. (presented 2000, July). *A survey of Key distribution*. Keynote presentation at 5th Annual Australasian Conference on Information Security and Privacy ACISP, Brisbane, International Association for Cryptological research, Australia. (International)

Burmester, M. (presented 2000, June). *Security over the Internet*. Keynote presentation at 5th Panhellenic Congress in Mathematical Education, Athens, Hellenic Mathematical Society, Greece. (National)

Invited Presentations at Conferences

Burmester, M. (presented 2013, July). *Lightweight RFID authentication with forward and backward security*. Presentation at 3rd Crypto.Sec Day, EU and Marie Curie Action IRG, Athens, Greece. (National)

Burmester, M. (presented 2013, June). *Trusted Clouds*. Presentation at DIMACS/BIC/A4Cloud/CSA International Workshop on Trustworthiness, Accountability and Forensics in the Cloud (TAFC), National Science Foundation, DIMACS, BIC, Malaga, Spain. (International)

Burmester, M. (presented 2012, March). *Modeling security in cyber-physical systems*. Presentation at Sixth Annual International Conference on Critical Infrastructure Protection, IFIP WG 11.10, National Defense University Fort McNair, Washington, DC, USA. (International)

Burmester, M. (presented 2010, June). *Network Profiling for High Assurance Survivability*. Presentation at MITACS Workshop on Network Security and Cryptography, Toronto, MITACS, Canada. (International)

Burmester, M. (presented 2010, June). *RFID and Ubiquitous applications - practical security for constrained devices*. Presentation at MITACS Workshop on Network Security and Cryptography, Toronto, MITACS, Canada. (International)

Invited Workshops

Burmester, M. (2016, January). *NSF Workshop for SaTC EAGER Grantees*. Workshop delivered at NSF and George Washington University, Washington, DC. (National)

Burmester, M. (2010, June). *RFID and Ubiquitous applications - practical security for constrained devices (One-day workshop course)*. Workshop delivered at MITACS Workshop on Network Security and Cryptography, Toronto, Canada. (International)

Invited Lectures and Readings of Original Work

Burmester, M. (2014, June). *Critical Infrastructure Resilience*. Delivered at University of the Ionian, Corfu, Greece. (International)

Burmester, M. (2014, March). *Reliable and Resilient Interdependent Infrastructure Systems*. Delivered at USA Center for Forensics, Information Technology and Security Lecture Series, Shelby Hall, University of South Alabama. (National) Retrieved from http://www.southalabama.edu/publicrelations/pressreleases/2014pr/03212014c.html

Burmester, M. (2012, May). *Trusted Computing: how can we trust our devices?* Delivered at Ionian University, Corfu, Greece. (National)

Burmester, M. (2011, June). *Private RFID localization*. Delivered at Schloss Dagstuhl, Leibnitz-Zentrum für Informatik, Wadern, Germany. (International)

Burmester, M. (2011, May). *His Late Master's Voice, Barking for location privacy*. Delivered at Ionian University, Corfu, Greece. (National)

Burmester, M. (2011, April). *Localization Privacy*. Delivered at MITACS International Focus Period, Carleton University, School of Computer Science, Ottawa. (International)

Burmester, M. (2010, June). *Network Profiling for High Assurance Survivability*. Delivered at Workshop on Network Security & Cryptography, Toronto, Canada. (International)

Burmester, M. (2010, June). *RFID and Ubiquitous applications: practical security for constrained devices --Short course*. Delivered at MITACS International Focus Period: Advances in Network Analysis & its Applications, Toronto, Canada. (International)

Burmester, M. (2010, May). *Cybersecurity*. Delivered at Ionian University, Corfu, Greece. (Local)

Burmester, M. (2010, May). *Cybersecurity: Defending our Digital Future*. Delivered at 3rd Annual TechExpo 2010, Tallahassee, Florida. (State)

Burmester, M. (2009, November). *Flyweight authentication with forward and backward security*. Delivered at WISP Summit, UC Berkeley, San Fransisco, Ca. (National)

Burmester, M. (2009, February). *Multi-Domain trust management in variable threat environments using rollback-access*. Delivered at Google Inc, Paramaribo Tech Talk 42, Mountain View, Ca. (Local)

Burmester, M. (2008, September). *Security for the Next Generation of Wireless Networks: the Good, the Bad, and the Evil*. Delivered at Florida Government Technology Conference, Tallahassee, Florida. (State)

Burmester, M. (2008, September). *The security of EPCGen2 compliant RFID protocols*. Delivered at FAMU-FSU College of Engineering, Tallahassee, Florida. (Local)

Burmester, M. (2008, April). *Persistent security in wireless applications*. Delivered at Ionian University, Corfu, Greece. (Local)

Burmester, M. (2008, April). *Secure Group Key Exchange*. Delivered at Ionian University, Corfu, Greece. (Local)

Burmester, M. (2008, March). *Persistent Security*. Delivered at Laboratory of Cryptography and Information Security, University of Tsukuba, Ibaraki, Japan. (State)

Burmester, M. (2008, February). *Information Security Institute: Strong Security for Feeble Devices*. Delivered at Queensland University of Technology, Brisbane, Australia. (State)

Burmester, M. (2007, October). *iCIS Distinguished Speaker: Persistent Security for RFIDs*. Delivered at University of Calgary, Calgary, Canada. (State)

Burmester, M. (2007, September). *iCIS Distinguished Speaker: Protecting ubiquitous applications: Beyond the Byzantine threats model*. Delivered at University of Calgary, Calgary, Canada. (State)

Burmester, M. (2007, September). *iCIS Distinguished Speaker: Provable security for route discovery in MANETs*. Delivered at University of Calgary, Calgary, Canada. (State)

Burmester, M. (2007, June). *Protecting ubiquitous applications*. Delivered at Ionian University, Corfu, Greece. (Local)

Burmester, M. (2006, November). *Lightweight, Uncloneable, Anonymous RFID Devices*. Delivered at Security Mobility Forum, NSA, Tampa, FL. (National)

Burmester, M. (2006, June). *Tracing malicious behavior in wireless mobile environments*. Delivered at 15th Mobile and Wireless Summit, Mykonos, Greece. (International)

Burmester, M. (2006, May). *The advent of trusted Computing: impact on digital forensics*. Delivered at Ionian University, Corfu, Greece. (Local)

Burmester, M. (2006, April). *Adaptive gossip protocols*. Delivered at School of Electrical Engineering, Cornell University, Ithaca, NY. (Local)

Burmester, M. (2006, March). *Reactive and Proactive approaches to Secure Routing in MANETs*. Delivered at NSF International Workshop on Research in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006), Miami, FL. (International)

Burmester, M. (2006, February). *Provable Security in wireless mobile networks*. Delivered at CERIAS, Purdue University, West Lafayette, Indiana. (Local)

Burmester, M. (2005, October). *Using wireless overlay networks for the secure management of network resources and to prevent extreme attacks*. Delivered at NATO Advanced Study Institute, Network Security and Intrusion Detection, Yerevan, Armenia. (International)

Burmester, M. (2005, May). *Computer Security, theory and peactice*. Delivered at University of the Ionian, Corfu, Greece. (Local)

Burmester, M. (2005, May). *Network Security, from models to practice*. Delivered at University of the Ionian, Corfu, Greece. (Local)

Burmester, M. (2004, July). *Trust Infrastructure Models for Mobile Environments*. Delivered at E-Business Forum: Trust and Confidence in a Fast and Mobile environment, Athens, Greece. (National)

Burmester, M. (2004, April). *Network Security?* Delivered at 6th Florida Communication Policy Symposium, College of Communication – FSU. (Local)

Burmester, M. (2004, February). *Security issues in ad hoc networks*. Delivered at University of Maryland, College Park, Maryland. (Local)

Burmester, M. (2003, May). *Group Key Exchange*. Delivered at Summer School on Information Security, SAIT Laboratory, Florida State University. (Local)

Burmester, M. (2002, November). *Securing Public Key Infrastructures*. Delivered at University of West Virginia, Morgantown WV. (Local)

Burmester, M. (2002, June). *Secret sharing and its application to distributed systems*. Delivered at Center for Secure Information Systems, George Mason University, Washington, DC. (Local)

Burmester, M. (2002, June). *Secure Role delegation for Mobile Agents*. Delivered at Center for Secure Information Systems, George Mason University, Washington, DC. (Local)

Burmester, M. (2000, August). *A tracing algorithm for the KD traceability Scheme*. Delivered at Queensland University of Technology, Brisbane, Australia. (State)

Burmester, M. (2000, August). *Security of Public Key Infrastructures*. Delivered at Queensland University of Technology, Brisbane, Australia. (State)

Burmester, M. (2000, June). *Strong Forward Secrecy*. Delivered at University of Wollongong, Wollongong, Australia. (Local)

Burmester, M. (1998, May). *Conference key Distribution systems*. Delivered at Tokyo Institute of Technology, Tokyo, Japan. (Local)

Burmester, M. (1998, May). *Trust and Security in Open Networks*. Delivered at TAO Telecommunications, Tokyo, Japan. (National)

Burmester, M. (1998, April). *Key Distribution*. Delivered at Japan Advanced Institute of Science and Technology, Kanasawa, Japan. (National)

Burmester, M. (1998, February). *Geometric Cryptography: Identification by angle trisection*. Delivered at University of Wisconsin, Milwaukee, WI. (Local)

Burmester, M. (1997, September). *Trust & Security: A new look at the Byzantine Generals Problem*. Delivered at Internationales Begegnungs und Forschungs Zentrum für Informatik (Cryptography), Schloss Dagstuhl, St Wadern, Germany. (International)

Burmester, M. (1996, November). *Trust and Security, The Byzantine Generals strike again, Security Group Seminar*. Delivered at Cambridge Computer Lab, Cambridge, England. (International)

Burmester, M. (1996, February). *Verifiable secret sharing*. Delivered at DIA, Saarland University, Saarbrücken. (National)

Burmester, M. (1995, September). *Multiplicative Sharing Schemes and Threshold Cryptography*. Delivered at Conference #916: Cryptography, Centre International de Rencontres Mathématiques (C.I.R.M.), Luminy, Marseille, France. (International)

Burmester, M. (1994, November). *Security measures in Information Theory*. Delivered at University of Piraeus, Greece. (Local)

Burmester, M. (1994, September). *Security problems in commercial key distribution systems*. Delivered at University of Wisconsin, Milwaukee , WI. (Local)

Burmester, M. (1994, March). *The protection of Information*. Delivered at University of Piraeus, Greece. (Local)

Burmester, M. (1993, September). *A Secure and Efficient Key Distribution System*. Delivered at Internationales Begegnungs und Forschungs zentrum für Informatik (Cryptography), Leibniz Center for Informatics (LZI), I Schloss Dagstuhl, St Wadern Germany. (International)

Burmester, M. (1993, June). *Recent developments in efficient zero-knowledge proofs*. Delivered at Recent developments in efficient zero-knowledge proofs – Université Catholique de Louvain, Louvain-la-Neuve, Belgium. (Local)

Burmester, M. (1992, October). *Practical vs. formal aspects of zero-knowledge proofs*. Delivered at University of Aarhus, Denmark. (National)

Burmester, M. (1992, March). *An efficient public key based authentication system*. Delivered at University of Wisconsin, Milwaukee, WI. (Local)

Patented Inventions

Burmester, M., van Le, T., de Medeiros, B., & Chatmon, C. (2014). *Systems, methods, and computer program products for secure optimistic mechanisms for constrained devices*. 8793496, FSU. Retrieved from http://www.uspto.gov/web/patents/patog/week30/OG/html/1404-5/US08793496-20140729.html

Burmester, M., & Van Le, T. (2010). *Method and system for generating and using digital fingerprints for electronic documents*. US 7,817,820 B2, FSU.

Contracts and Grants

Contracts and Grants Funded

Burmester, M., & Liu, X. (Sep 2017–Sep 2018). *Integrating Hands-on Offensive Security Labs and Learning Experiences into Cybersecurity"*. Funded by NSA/DHS. (S-004-2017). Total award $289,027.

Burmester, M., Liu, X., Whalley, D., & Yang, Y. (Aug 2016–Jul 2021). *Renewal: Cybercorps: Scholarship for Service at FSU*. Funded by National Science Foundation. (DGE 1565215). Total award $4,599,546.

Burmester, M., & Liu, X. (Sep 2015–Sep 2016). *A Resiliency Framework for Electrical Grids based on Vulnerability Analysis and HIL Testing*. Funded by NSA/DHS. (BAA-003-15). Total award $291,312.

Burmester, M., Whalley, D., & Hay, C. (Mar 2015–Sep 2017). *Scholarships for Service for FSU MS CC and CNSA Students (supplement)*. Funded by National Science Foundation. (NSF DGE 1538850). Total award $300,400.

Burmester, M., & Liu, X. (Sep 2013–Sep 2014). *Secure Cyber Physical Systems for Critical Infrastructure Protection*. Funded by NSA/DHS, DoD Information Assurance - Information Security Program. (H98230-13-1-0410). Total award $53,342.

Burmester, M., Whalley, D., Hay, C., & Liu, X. (Sep 2013–Sep 2017). *Scholarships for Service for FSU MS CC and CNSA Students, at Florida State University*. Funded by National Science Foundation. (NSF DUE 1241525). Total award $2,224,096.

Ho, S., Burmester, M., & Liu, X. (Sep 2013–Sep 2015). *EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication*. Funded by National Science Foundation. (NSF 1347113). Total award $119,998.

Burmester, M., & Liu, X. (Sep 2012–Dec 2013). *Scholarships for Information Assurance and Security at FSU*. Funded by National Security Agency. Total award $38,984.

Caballero, Pino Gil (PI), Arranz, C., Burmester, Mike (US Investigator), Fuster, S., Hernandez, G., Herrera, P., Martin del Rey, Felix, & Molin Jill, J. (Jan 2012–Dec 2014). *TUERI: Technologias seguras y eficientes para las redes inalambricas en la Internet de las cosas con applicationes en transporte y logistica*. Funded by Ministero de Ciencia e Innovacion and FEDER (European fund for regional development). (TIN2011-25452). Total award $106,516.

Burmester, M., & Whalley, D. (Sep 2011–Dec 2012). *Scholarships for Information Assurance and Security at FSU*. Funded by National Security Agency (Information Assurance Scholarship Program). Total award $19,325.

Burmester, M., Liu, X., Aggarwal, S., & Li, F. (Sep 2010–Aug 2014). *Scholarships for Service at Florida State University*. Funded by National Science Foundation. (NSF DUE 1241525). Total award $1,853,894.

Burmester, M., & Whalley, D. (Sep 2010–Dec 2011). *Scholarships for Information Assurance and Security at FSU*. Funded by National Security Agency (Information Assurance Scholarship Program). Total award $29,584.

Burmester, Mike (PI), & Li, F. (Aug 2009–Dec 2010). *DoD Information Assurance Scholarship Program*. Funded by National Security Agency. Total award $46,997.

Burmester, Mike (PI). (May 2009–Jun 2012). *Harris Professorship*. Funded by FSU Foundation. Total award $4,065.

Burmester, Mike (PI). (Nov 2008–Jun 2009). *Sait Lab*. Funded by FSU Foundation. Total award $10,000.

Yasinsac, Alec F (PI), Burmester, M., & De Medeiros, B. F. (Sep 2007–Sep 2008). *Scholarships for Security and Assurance in Info Techn*. Funded by U. S. Department of Defense. Total award $197,182.

Burmester, Michael V D (PI). (Aug 2006–Jan 2007). *NPSC Fellowship - Christopher Moss*. Funded by National Physical Science Cons. Total award $8,000.

Burmester, Mike (PI), & Yasinsac, A. F. (Aug 2006–Nov 2007). *Scholarships for Security and Assurance*. Funded by National Security Agency. Total award $147,049.

Burmester, Mike (PI). (Jul 2006–Jul 2007). *Pacer D2 WSN*. Funded by Johns Hopkins University. Total award $33,913.

Aggarwal, Sudhir (PI), Yasinsac, A. F., & Burmester, M. (Oct 2004–Jun 2006). *The Design and Development of the Predator and Prey*. Funded by National Institute of Justice. Total award $280,998.

Yasinsac, Alec F (PI), & Burmester, M. (Oct 2004–Sep 2007). *Security in Mobile Agents*. Funded by Florida A&M University. Total award $69,447.

Burmester, Mike (PI). (Aug 2004–Sep 2006). *Mentoring of EWC Research Group Establishment*. Funded by Edward Waters College. Total award $25,000.

Burmester, Mike (PI), & Yasinsac, A. F. (Aug 2004–Dec 2006). *Scholarships for Security and Assurance in Information*. Funded by National Security Agency. Total award $436,469.

Yasinsac, Alec F (PI), & Burmester, M. (Jul 2004–Dec 2005). *Workshop on Security in Mobile Agents and Sensor Network*. Funded by U. S. Army Research Laboratory. Total award $11,700.

Yasinsac, Alec (PI), Burmester, M., & Desmedt, Y. (Sep 2003–Oct 2006). *Collaborative Project: Expanding Information Assurance Education*. Funded by National Science Fundation. (0313860). Total award $185,405.

Burmester, Mike (PI), & Yasinsac, A. (Jan 2003–Aug 2007). *Cyber Training and Education at Florida State University*. Funded by National Science Foundation. (0243117). Total award $1,348,680.

Desmedt, Yvo (PI), & Burmester, M. (Aug 2002–Jul 2007). *Models for Trusted Systems*. Funded by National Science Foundation. (CCR-0209092). Total award $291,297.

Burmester, Mike (PI), & Yasinsac, A. F. (Jul 2002–Jul 2005). *Secure TActical Mobile INtelligent Agents (STAMINA)*. Funded by Army Research Office. Total award $196,055.