

BRENO F. DE MEDEIROS

P. O. Box 1049
Tallahassee, FL 32302-1049
Phone: (850) 339-8951

Fax: (815) 346-5174
E-mail: breno@brenodemedeiros.com
URL: www.brenodemedeiros.com

Education

Ph. D. in Computer Science, Johns Hopkins University, Baltimore MD.

Sep. 1999 – May 2004.

Thesis topic: New Cryptographic Primitives with Applications to Information Privacy and Corporate Confidentiality.

M. S. in Security Informatics, The Johns Hopkins University, Baltimore MD.

May 2003.

M. A. in Mathematics, The Johns Hopkins University, Baltimore MD.

May 1994.

M. S. in Mathematics, Universidade Federal de Pernambuco, Recife, Brazil.

Aug. 1993.

Graduated with Honors.

B. S. in Mathematics, Universidade Federal de Pernambuco, Recife, Brazil.

Mar. 1989 – Jun. 1992.

Refereed

Publications

[BdM07b] M. Burmester and B. de Medeiros. Persistent Security for RFID. *Proceedings of the Conference on RFID Security 07 (RFIDSec'07)*, July, 2007, Málaga, Spain. To appear.

[ABD⁺07] S. Aggarwal, D. Beech, R. Das, B. de Medeiros, and E. Thompson. X-Online: An Online Interface for Digital Decryption Tools. *Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE), 2007*, pages 105–116, 2007.

[vLBdM07] T. van Le, M. Burmester, and B. de Medeiros. Universally composable and forward-secure RFID authentication and authenticated key exchange. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007)*. ACM Press, 2007.

[BdM07a] Mike Burmester and Breno de Medeiros. RFID security: Attacks, countermeasures and challenges. In *Proceedings of the RFID Journal Live! Conference*, 2007.

**Refereed
Publications**

[BvLdM06a] M. Burmester, T. van Le, and B. de Medeiros. Provably secure ubiquitous systems: Universally composable rfid authentication protocols. In *Proceedings of the 2nd IEEE/CreateNet International Conference on Security and Privacy in Communication Networks (SECURECOMM 2006)*. IEEE Press, 2006.

[BvLdM06b] M. Burmester, T. van Le, and B. de Medeiros. Towards provable security for ubiquitous applications. In *Proceedings of the 11th Australasian Conference on Information Security and Privacy (ACISP 2006)*, volume 4058 of *Lecture Notes in Computer Science*, pages 295–312, 2006.

[ACdM05] G. Ateniese, J. Camenisch, and B. de Medeiros. Untraceable RFID tags via insubvertible encryption. *Proceedings of the 12th ACM conference on Computer and communications security*, pages 92–101, 2005.

[ACdMT05] G. Ateniese, D.H. Chou, B. de Medeiros, and G. Tsudik. Sanitizable signatures. *ESORICS: Proceedings of the 10th European Symposium on Research in Computer Security*, 3679:159–ff., 2005.

[KdMW05] S. Kamara, B. de Medeiros, and S. Wetzel. Secret Locking: Exploring New Approaches to Biometric Key Encapsulation. *Proceedings of the 2nd International Conference on e-Business and Telecommunications (ICETE 2005)*, 2005.

[AdM04a] G. Ateniese and B. de Medeiros. Identity-based chameleon hash and applications. *Proceedings of Financial Cryptography (FC'04)*, 3110:164–180, 2004.

[AdM04b] G. Ateniese and B. de Medeiros. On the Key Exposure Problem in Chameleon Hashes. *Proceedings of the Fourth Conference on Security in Communication Networks (SCN'04)*, 3352:165–, 2004.

[AdM03] G. Ateniese and B. de Medeiros. Efficient group signatures without trapdoors. *Advances in Cryptology—ASIACRYPT*, 2894:246–268, 2003.

[AdM02] G. Ateniese and B. de Medeiros. Anonymous E-prescriptions. *Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society (WPES'02)*, pages 19–31, 2002.

[ACdMD02] G. Ateniese, R. Curtmola, B. de Medeiros, and D. Davis. Medical Information Privacy Assurance: Cryptographic and System Aspects. *Third Conference on Security in Communication Networks (SCN'02)*, pages 12–13, 2002.

[AdMG01] G. Ateniese, B. de Medeiros, and M.T. Goodrich. Tricert: Distributed certified e-mail schemes. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'01)*. Internet Society (ISOC), 2001.

**Other
Publications**

[BdM07] M. Burmester and B. de Medeiros. Towards Provable Security for Routing Protocols in Mobile ad Hoc Networks. *Cryptology ePrint Archive, Report 2007/324*, <http://eprint.iacr.org>. IACR, 2007.

[YWB⁺07] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester. Software review and security analysis of the ES&S iVotronic 8.0.1.2 voting machine firmware. *Technical report, Florida Department of State, Division of Elections*, 2007, available at <http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf>.

[BvLdMT07] M. Burmester, T. van Le, B. de Medeiros, and G. Tsudik. Universally Composable RFID Authentication Protocols. Submitted, 2007.

[ACHdM05] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical group signatures without random oracles. In *Cryptology ePrint Archive, Report 2005/385*, <http://eprint.iacr.org>. IACR, 2005.

[BGdMM05] L. Ballard, M. Green, B. de Medeiros, and F. Monrose. Correlation-Resistant Storage via Keyword-Searchable Encryption. In *Cryptology ePrint Archive, Report 2005/417*, <http://eprint.iacr.org>. IACR, 2005.

[AdM04c] G. Ateniese & B. de Medeiros, A Provably Secure Nyberg-Rueppel Signature Variant with Applications. In *Cryptology ePrint Archive, Report 2004/093*, <http://eprint.iacr.org>. IACR, 2005.

[dM04] Breno de Medeiros. New Cryptographic Primitives with Applications to Information Privacy and Corporate Confidentiality. *Ph.D. Thesis, Johns Hopkins University, Baltimore, Maryland*, 2004.

Patents

[AdMG00] G. Ateniese, B. de Medeiros, & M. T. Goodrich. *Intermediated Delivery Scheme for Asymmetric Fair Exchange of Electronic Items*. US Patent Serial#: 60/218,172. Filing date: 7/14/2000.

[BCvLdM06] M. Burmester, C. Chatmom, T. van Le, and B. de Medeiros. *Systems, methods, and computer program products for secure optimistic mechanisms for constrained devices*. Pending.

**Conference
Presentations**

- *Persistent Security for RFID*. International Conference on RFID Security (RFIDSec 2007). Málaga, Spain. July, 2007.

- *Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols*. 2nd Annual IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2006). Baltimore, Maryland. September, 2006.

Conference Presentations

- *Untraceable RFID Tags via Insubvertible Encryption*. Presented at ACM Conference on Computer and Communication Security (ACM CCS 2005), Washington, D.C. October, 2005.
- *The XDH Assumption*. International Workshop on Pairings in Cryptography (PiC 2005). Dublin City University, Dublin, Ireland. June, 2005.
- *Community-centric authentication with vanilla-rollback access, or: How I stopped worrying and learned to love my computer*. 13th International Workshop on Security Protocols. Cambridge, UK, April 2005.
- *Efficient Group Signatures without Trapdoors*. Presented at the IACR Advances in Cryptology Conference – ASIACRYPT 2003, Taipei, Taiwan. December, 2003.

Invited Talks

- *RFID: Strong Security for Feeble Devices?* To be presented at ADHOC-NOW: 6th International Conference on Ad Hoc Networks and Wireless, Morelia, Mexico, September 2007.
- *Providing Accountable Anonymity in Ad-hoc Groups*. Keynote Talk. Carleton Wireless Security Day, Carleton University, Ottawa, Canada, March 2007.
- *Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols*. Computer Science Seminar Series, Carleton University, Ottawa, Canada, October 2006.
- *Untraceable RFID tags via insubvertible encryption*. Presented at the National Institute of Standards and Technology (NIST) Colloquium Series. Bethesda, Maryland, October 2005.
- *Cryptography*. Invited Lecture. Faye Jones, Instructor. School of Law, Florida State University, March 2005.
- *The XDH Assumption*. Johns Hopkins University Security and Privacy Applied Research Seminar Series. Baltimore, Maryland. Oct. 2004.
- *Group Signatures Mean Privacy*. George Mason University Computer Science Seminar, Fairfax, Virginia. April, 2004.
- *Group Signatures Mean Privacy*. Florida State University Computer Science Seminar, Tallahassee, Florida. March, 2004.
- *Group Signatures Mean Privacy*. The Stevens Institute of Technology Computer Science Seminar Series, Hoboken, New Jersey. February, 2004.
- *Medical Information Privacy Assurance*. Presented at Johns Hopkins Information Security Institute (JHUISI) Open House, Baltimore MD, Oct. 2001.

**Conference
Service**

PC Member, *NPsec 2007: Third Workshop on Secure Network Protocols*. October 16, 2007, Beijing, China.

PC Member, *ISC 2007: Information Security Conference*, October 9–12, 2007, Valparaíso, Chile.

PC Member, *AdHoc Now 2007: Sixth International Conference on Ad-Hoc Networks and Wireless*. September 24-26, Morelia, Mexico.

PC Member, *SECRYPT 2007: International Conference on Security and Cryptography*. July 28-31, Barcelona, Spain.

PC Member, *SecPerU 2007: 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing*. July 20, 2007, Istanbul, Turkey.

PC Member, *Securecomm 2006: Second IEEE Communications Society / CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks*. Baltimore, United States, September 2006.

PC member, *NPsec 2006: Second Workshop on Secure Network Protocols*. Santa Barbara, California, November 2006.

PC Member, *ESAS 2006: Third European Workshop on Security and Privacy in Ad Hoc and Sensor Networks*. Hamburg, Germany, September 2006.

PC Member, *SBSeg 2006: Sixth Brazilian Symposium on Information and Computer System Security*. Santos, Brazil, September 2006.

PC Member, *TSPUC 2006: IEEE International Workshop on Trust, Security and Privacy for Ubiquitous Computing*. Niagara-Falls, NY, USA, June 2006.

PC Member, *ACMSE 2006: 44th ACM Southeast Conference*. Melbourne, FL, March 2006.

General Co-Chair & PC Member, *Secure MADNES 2005: International Workshop on Secure Mobile Ad-hoc Networks and Sensors*. Singapore, September 2005.

PC member, *ESAS 2005: 2nd European Workshop on Security and Privacy in Ad hoc and Sensor Networks*, July 2005, Budapest, Hungary.

PC member, *PSC 2005: International Conference on Pervasive Systems and Computing*. June 2005, Las Vegas, Nevada.

PC member, *WWW 2004: Security and Privacy Track*. May 2004, New York, New York.

Reviews

ACNS 2007: *International Conference on Applied Cryptography and Network Security*, June, 2007, Zhuhai, China. ICNP 2007: *Fifteenth IEEE International Conference on Network Protocols*, October 16–19, 2007, Beijing, China. Book draft, William Stallings, *Computer Security*, Prentice Hall, 2007. *Information Processing Letters*, Masafumi Yamashita, editor, 2006. *ACM Transactions on Information and System Security (TISSEC)*, Mike Reiter, editor, 2006. *Journal of Mathematical Cryptology*, Mike Burmester, editor, 2006. ICICS 2006: *Eighth International Conference on Information and Communications Security*, November, 2006, Raleigh, North Carolina. ACM CCS 2006: *ACM Conference on Computer and Communications Security*, October, 2006, Arlington, Virginia. PKC 2006: *9th International Workshop on Practice and Theory in Public Key Cryptography*, April, 2006, New York, New York. FC 2006: *10th International Conference on Financial Cryptography and Data Security*, February, 2006, Anguilla, British West Indies. *IEEE Transactions on Computers*, Mikhail Atallah, editor, 2005. WWW 2005: *The 14th International World Wide Web Conference*, May, 2005, Japan. Book draft, W. Stallings, *Cryptography and Network Security, Principles and Practices*, 4th edition draft, 2005, Prentice Hall. ISCC 2005: *The 10th IEEE Symposium on Computers and Communications*, June, 2005, Spain. WISA 2003: *Workshop on Information Security Applications*, August 2003, Jeju Island, Korea. CCS 2003: *ACM Conference on Computer and Communications Security*, October, 2003, Washington, D.C. RSA 2003: *Cryptographer's Track*, April, 2003, San Francisco, CA.

Funded Projects

FSU Research Foundation: *Systems, methods, and computer program products for secure optimistic mechanisms for constrained devices*, 11/2006–10/2007.

PI: Mike Burmester. Co-PI: Breno de Medeiros.

Amount: \$40,000.00

Florida Department of State: *Software review and security analysis of the ES&S iVotronic voting machine firmware*, 11/06–06/07.

PI: Alec Yasinsac. Co-PIs: Breno de Medeiros & Mike Burmester.

Amount: \$ 157,000.00

Department of Defense: *Information Assurance Scholarship Program*, 06/2005–05/2007.

PI: Mike Burmester. Co-PIs: Breno de Medeiros, Alec Yasinsac.

Amount: \$264,735.00.

FSU Council on Research and Creativity: *Privacy in the Context of Ubiquitous Computing*, 05/08/2006–04/30/2007.

PI: Breno de Medeiros.

Amount: \$9,936.95

- Funded Projects** FSU Council on Research and Creativity: *First-Year Assistant Professor Award*, 05/09/2005–08/05/2005.
PI: Breno de Medeiros.
Amount: \$14,000.00
- Advising** William Glodek, *Digital Forensics Tool Using Information Retrieval Techniques*, Masters thesis, current. Rossana Motta, *RFID Security Protocols*, Master thesis, current (Ph. D. student candidate). Arjun Roy, *Password and Passphrase Cryptanalysis*, Master thesis, current (Ph. D. student candidate). Kenneth Zahn, *Design and Implementation of Applied Computer Security Laboratory Exercises in Linux and Windows*, Masters project, FSU, Fall 2006. James Coppens, *PrivRX: Cryptographic Application Software*, Masters project, Spring 2006.
- Awards** **Outstanding Teaching** Award, by the JHU Computer Science Department. For teaching a new undergraduate course “Introduction to Cryptography” and for services to the department as a Teaching Assistant. 2004.
- Professional Memberships**
- Association for Computing Machinery (ACM).
 - Institute of Electrical and Electronics Engineers (IEEE).