

# CURRICULUM VITAE

## TRI VAN LE

Department of Computer Science, 253 Love Building  
Florida State University, Tallahassee, Florida 32306-4530, USA.  
Phone: (850) 345-6468, Fax: (850) 644-0058.  
E-mail: [levan@cs.fsu.edu](mailto:levan@cs.fsu.edu).

**Current Position:** Assistant Scholar Scientist, Florida State University.

**Research Interests:** Information, Media, Wireless, and Software Security.

### Education

---

Doctor	Doctor of Philosophy in Computer Science, Florida State University, USA Dissertation: Information Hiding, May 2004.
Master	Master in Computer Science, University of Wisconsin, Milwaukee, USA Thesis: Covert Cryptography, August 1999.
Bachelor	Bachelor in Computer Science, Vietnam National University, Vietnam Thesis: Algorithms on Monomial Curves, May 1997.

### Honors and Awards

---

2002	Southeast Finalist, Sun Microsystems Top-coder Collegiate Challenge, 2002.
2001	Academic Excellence Award, UPE, ACM and IEEE Computer Society, 2001.
1994	First Prize, National Olympiads in Informatics, Hanoi, Vietnam, April 1994.
1994	Merit Award, Fund for young Talents of Vietnam, April 1994.
1994	Third Prize, National Olympiads in Algebra, Hanoi, Vietnam, June 1994.
1994	Encouraging Prize, National Olympiads in Analysis, Hanoi, Vietnam, June 1994.
1993	First Prize, National Olympiads in Informatics, Hanoi, Vietnam, April 1993.
1993	Second Prize, National Olympiads in Mathematics, Hanoi, Vietnam, June 1993.
1992	Third Prize, International Olympiads in Informatics, Bonn, Germany, July 1992.
1990	Mathematics and Informatics Merit Award, Hanoi, Vietnam, December 1990.

### Professional Membership

---

Member of Association of Computing Machinery.

Member of IEEE Computer Society.

## Selected Publications

---

- 2007      *Universally Composable and Forward Secure RFID Authentication and Authenticated Key Exchange*. Tri Van Le, Mike Burmester and Breno de Medeiros. ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), Singapore, March 2007. **(17.6% acceptance rate)**
- 2006      *Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols*. Mike Burmester, Tri Van Le, Breno de Medeiros. Proceedings of 2nd International IEEE Conference in Security and Privacy in Communication Networks (SECURECOMM 2006), Baltimore, MD, USA, August 28 - September 1, 2006. **(25% acceptance rate)**
- 2006      *Towards Provable Security for Ubiquitous Applications*. Mike Burmester, Tri Van Le, Breno de Medeiros. Proceedings of 11th Australian Conference on Information Security and Privacy (ACISP 2006), pp. 295-312, Melbourne, Australia, July 2006. LNCS 4058, Springer Verlag. **(26% acceptance rate)**
- 2004      *Weathering the storm: managing redundancy and security in ad hoc networks*. Mike Burmester and Tri Van Le and Alec Yasinsac. Proceedings of the 3rd International Conference on Wireless and Ad hoc networks (ADHOC-NOW 2004), Vancouver, British Columbia, pp. 96-107, July 22-24, 2004. LNCS 3158, Springer Verlag. **(17% acceptance rate)**
- 2003      *Short  $c$ -secure Fingerprinting Code*. Tri Van Le and Mike Burmester and Jiangyi Hu, Proceedings of 6th Information Security Conference 2003 (ISC 2003), pp. 422-427, Bristol, England. LNCS 2851, Springer Verlag, 2003. **(23% acceptance rate)**
- 2003      *Error Correcting and Complexity Aspects of Linear Secret Sharing Schemes*. Yvo Desmedt and Kaoru Kurosawa and Tri Van Le. Proceedings of 6th Information Security Conference 2003 (ISC 2003), pp. 396-407, Bristol, England. LNCS 2851, Springer Verlag, 2003. **(23% acceptance rate)**
- 2002      *Moire Cryptography*. Yvo Desmedt and Tri Van Le, 7th ACM Conference on Computer and Communications Security 2000 (ACM CCS 2000), pp. 116-124, Athens, Greece. ACM Press 2002. **(21% acceptance rate)**

## Journal Articles

---

- 2005      *Adaptive Gossip Protocols: managing redundancy in dense ad hoc networks*. Mike Burmester and Tri Van Le and Alec Yasinsac. Journal of Ad hoc networks, Elsevier, 2007, Volume 5, Issue 3, pp 286-297.
- 2004      *Attack on Sebe, Domingo-Ferrer and Herrera-Joancomarti fingerprinting schemes*. Mike Burmester and Tri Van Le, IEE Electronic Letters, pp. 172-173, Vol. 40, Issue 3, February 2004.
- In review      *Remarks on Entity Authentication*. Tri Van Le and Mike Burmester. Preprint, Information Processing Letters, IEEE, 2006.

- In review *Optimistic Fault Tracing and Secure Adaptive Multipath Routing in MANETs*. Tri Van Le and Mike Burmester. Journal of Wireless Networks. Springer Verlag. 2006.
- In review *Universally Composable RFID Authentication Protocols*. Mike Burmester, Tri Van Le, Breno de Medeiros, and Gene Tsudik. ACM Transactions on Information and System Security.

## Refereed Publications

---

- 2006 *Efficient Public Key Steganography Secure Against Adaptive Chosen Stegotext Attacks*. Tri Van Le and Kaoru Kurosawa. Proceedings of the 8<sup>th</sup> International Conference on Information Hiding (IH2006), Washington DC, USA, July 2006. Preliminary version available as IACR Technical Report 2003/244, November 2003.
- 2006 *Secure anonymous RFID authentication protocols*. Christy Chatmon, Tri Van Le and Mike Burmester. Technical Report TR-060112, Department of Computer Science, Florida State University, Tallahassee, Florida, USA, 2006.
- 2006 *Reactive and Proactive Approaches to Secure Routing in MANETs*, Mike Burmester and Tri Van Le, Proceedings of International Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN'06), Miami, USA, March 2006.
- 2005 *Security Issues in Mobile Ad hoc Networks (Book Chapter)*. Mike Burmester and Tri Van Le. Network Security (Book), Scott Huang, David MacCallum, and Ding Zhu Du (Editors). Springer Verlag, In Printing, November 2005.
- 2004 *Complementation-like and Cyclic properties of AES Round Functions (Invited Paper)*. Tri Van Le and Rudiger Sparr and Ralph Wernsdorf and Yvo Desmedt. Proceedings of 4<sup>th</sup> International Conference on Advanced Encryption Standard (AES 2004), pp. 128-141, May 2004, Bonn, Germany. LNCS 3373, Springer Verlag, 2005.
- 2004 *Secure Communications in Ad hoc networks*, Mike Burmester and Tri Van Le. Proceedings of 5<sup>th</sup> Annual IEEE Information Assurance Workshop (IAW 2004), USMA, West Point, New York, pp. 234-241, June 2004.
- 2003 *Secure Multipath Communication in Mobile Adhoc Networks*, Mike Burmester and Tri Van Le. Proceedings of IEEE International Conference on Information Technology: Coding and Computing (ITCC 2004), Vol. 2, pp. 405-409, Las Vegas, USA, April 5-7, 2004.
- 2003 *Tracing Byzantine Faults in Ad Hoc Networks*, Mike Burmester and Tri Van Le and Matt Weiss. Proceedings of IASTED International Conference on Communication, Network, and Information Security 2003 (CNIS 2003), pp. 105-108, ACTA Press, New York, USA, 2003.
- 2003 *Efficient Provably Secure Public Key Steganography*. Tri Van Le. IACR Cryptology Archive, Technical Report 2003/156, November, 2003.

- 2002 *Cryptanalysis of UCLA Watermarking Schemes for Intellectual Property Protection*, Tri Van Le and Yvo Desmedt, 5th International Workshop in Information Hiding 2002 (IH 2002), pp. 213-225, Noordwijkerhout, The Netherlands. LNCS 2578, Springer Verlag 2002.
- 1999 *Nonbinary Audio Cryptography*, J.-J. Quisquater and Yvo Desmedt and Tri Van Le, 2nd International Workshop on Information Hiding 1999, Dresden, Germany. Springer Verlag 1999.
- 1999 *How To Prove That a Committed Number Is Prime*. Tri Van Le and Khanh Nguyen and Vijay Varadharajan. *Advances in Cryptology, Proceedings of 6<sup>th</sup> International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 1999)*, Singapore, November 14-18, 1999. LNCS 1716, pp. 208-218, Springer Verlag.
- 1998 *Incremental Constraint-Based Elicitation of Multi-Attribute Utility Functions*, Tri Van Le and Peter Haddawy. *AAAI Symposium on Interactive and Mixed-Initiative Decision-Theoretic Systems*, Stanford University, California, 1998. ISBN 978-1-57735-048-4.
- 1998 *Case-Based Preference Elicitation*, Vu Ha and Tri Van Le and Peter Haddawy, *AAAI Symposium on Interactive and Mixed-Initiative Decision-Theoretic Systems*, Stanford University, California, 1998. ISBN 978-1-57735-048-4.
- 1996 *Normal form computation for cubic curves*, Tri Van Le, *International Conference on Algebra, Geometry, and Computer Algebra*, Hanoi Institute of Mathematics, Hanoi, August 19-23, 1996.

## Patents

---

- 2006 Co-inventor: Systems, Methods, and Computer Program Products for Secure Optimistic Mechanisms for Constrained Devices. Applied for Patent, United States Patent and Trademark Office, August 2006. Application No 60/822,765.
- 2004 Co-inventor: A Method of Inserting Digital Fingerprints into Electronic Documents which is Resistant to Manipulations. Applied for Patent, United States Patent and Trademark Office, 2004. Application No 10/998,299.

## Professional Services

---

- Referee *Designs, Codes and Cryptography*, Springer Press.
- The Computer Journal*, British Computer Society, Oxford University Press.
- IEEE Transactions on Information Theory*, IEEE Information Theory Society.
- IEEE Transactions on Information Forensics and Security*, Signal Processing Society.
- IEEE Transactions on Computers*, IEEE Computer Society.
- IEICE Transactions on Fundamentals of Electronics, Communications and Computer*

Sciences, The Institute of Electronics, Information and Communication Engineers.

International Journal of Communications in Information and Systems, The Institute of Mathematical Sciences, International Press.

Committee Mobile Ad hoc Networks and Sensors 2005.

## **Research Experiences**

---

- 2006-present Assistant Scientist, Department of Computer Science, Florida State University.
- 2004-2005 Visiting Scholar, Department of Computer Science, Florida State University.
- 2000-2004 Research Assistant, Cryptography Laboratory, Florida State University.
- 1998-1999 Research Assistant, Cryptography Laboratory, University of Wisconsin.
- 1997-1998 Research Assistant, Decision Support System Laboratory, University of Wisconsin.

## **Teaching Experiences**

---

- 2004 Florida State University, USA  
Introduction to Network Security (undergraduate).  
Introduction to Computer Security (undergraduate).
- 2003 Florida State University, USA  
Introduction to Java Programming (undergraduate).
- 1999 University of Wisconsin at Milwaukee, USA  
Introduction to C++ Programming (undergraduate).