

Tieyan LI (*Terry*)

Contact Address

#21-01 Connexis,
1 Fusionopolis Way,
Singapore 138632

Phone: (65) 64082038
Fax: (65) 64669302
Email: litieyan@gmail.com

Summary

- * Research on **Security and Applied Cryptography** in various applications.
- * In depth understanding of specific IT security technologies supporting multi-tiered network systems.
- * More than 10-year experiences on IT system analysis and development with various computer platforms, languages and networks.
- * Project management, business development, communication skills.
- * Energetic, responsible, cooperative and quick-learning.

Education

[Dec. 1998 — Oct. 2001] National University of Singapore

Major: Cryptography and Network System Security

Degree: Ph.D. of Computer Science (May 2003)

[Sep. 1990 — Jul. 1994] Nan Kai University, Tianjin, China

Major: 1. Computer Software 2. Electronics and Information Systems

Dual-Degree: B.Sc. of CS and B.Sc. of EIS

Research Experiences [1999 - Present]

[Oct. 2001 - Now] **Principal Investigator & Senior Research Fellow, Cryptography and Security Dept., Institute for InfoComm Research (I^2R), A*Star, Singapore**

My ruling passion is on security research in various applications, for which I understand the security requirements, design security systems and develop the prototypes. Refer to appendix for my recent publications.

Current funded projects:

- ◇ A Security Framework for EPCglobal Network. (*Co-PI, A*star Public Sector Funding, S\$479K, Aug. 2008-Aug. 2011*)
- ◇ Real-Time Secure RFID-Based Track and Trace in Aerospace MRO Supply Chain. (*Co-PI, A*star Aerospace program (security part), S\$523K, Jan. 2009-Jan. 2011*)
- ◇ Wireless communication with medical implants - design of new PHY layer for in-body medical diagnostic. (*Co-PI, A*star MEDTECH program (security part), S\$700K, Sept. 2008-Sept. 2011*)

Former projects:

- ◇ Privacy Protection in RFID Systems. (*04/2007-03/2009, Research collaboration project with Kyushu Univ. Japan, A*Star Co-funding*)

- ◇ Secure and real-time RFID based track and trace information management in EPCglobal-enabled supply chains. (*05/2007-10/2008, Joint Research Project: I²R-SIMtech, A*Star funding*)
- ◇ SenSec: A more secure and efficient link layer sensor security framework (*A*star flagship project on sensor network 2004-05*)
- ◇ mSSA: A flexible MPEG-4 authentication framework, a complementary for multimedia DRM solutions. (*A*star core project 2003-04*)
- ◇ Disruptive security issues in *P2P, Grid, Trust Computing, VoIP, WWW, Tamper-resistant software/hardware, etc.*

[Jan. 1999 - Oct. 2001] Ph.D. Candidate, School of Computing, National University of Singapore

I pursued my Ph.D. study at NUS with research topics on cryptography and network security. I focused on “intrusion detection using mobile agent techniques” while exploring various cryptographic algorithms, protocols and architectures as well as tools.

1. Projects: *Secure Agent-mediated E-Commerce* and *WAP compatible Wireless Open Standard*.
2. Design and implement project/thesis *Building secure mobile agent architecture for intrusion detection*.

Working Experiences [1994 - 1998]

[Apr. 1998 - Dec. 1998] Chief-Engineer, NewPost Computer Pte. Ltd., China

I joined a startup as a chief-engineer, where I managed 20⁺ engineers and worked for network integration and database development projects. Beyond a technical role, I had also taken part in business development, sales and marketing.

1. Consultant for *wireless billing system with software & network solutions*.
2. Design *GPS real time control, audit and schedule network for automobile management*.

[Dec. 1997 - Apr. 1998] Senior Engineer, System Design Department of AsiaInfo Corp., China

At the system design dept. of AsiaInfo, one of the earliest high-tech companies in China IPOed (ASIA) on NASDAQ, I was mainly responsible for large scale network design of ChinaNet and partially supporting pre-sales, post-sales and marketing.

1. Consultant for *Large scale network design and system analysis for ChinaNet-II backbone network*. (*www.163.net*)
2. Design and develop *the billing software for China public multimedia network*. (*www.169.com*)

[Jun. 1994 - Dec. 1997] Software Engineer, R&D center, North China Institute of Computing Technology, China

Freshly graduated, I joined the R&D center of NCI as a software engineer. I participated in several national key projects, in which I was technically enriched in several aspects like software development, network administration and security assessment.

1. *National Key Projects - Computer Network Test System & Ruggedized computer system (Jun. 1994-Dec. 1996)*
2. *Computerized Finance Network System Integration & Message Handling System (Mar. 1995-Dec. 1997)*

Inventions

[Jun. 2003] **Rcrypto – PCT NO. WO 2005/034423 A1, SG NO. 120791**
“*Resilient Public Key Cryptographic System*” with A. Lux, F. Bao, R. Deng. And in news: **The RCrypto vaccine** in COMPUTERWORLD-Singapore, Vol. 10, Issue No. 13, 18-24 February 2004.

[Jul. 2006] **RFID Anti-Counterfeiting Series, PCT NO. WO 2008/085135 A1.**

“*Methods and Systems of Marking and Verifying An Information Tag*”. with Y. Wu, W. He, P.S. Tan, T.L. Lim. US Provisional (Jan. 2007- Jan. 2008), Filed for US patent on Jan. 2008.

- “*Method on protecting EPC RFID tags against counterfeiting*”
- “*Method on protecting a batch of EPC RFID tags*”
- “*Method on protecting a set of undetachable EPC RFID tags*”
- “*An invisible marking scheme for the verification of EPC RFID tags*”
- “*Privacy enhanced tag protection method for secure RFID supply chain*”

Professional

Adjunct Assistant Professor:

-School of Information System, Singapore Management University (2008-2011)

Steering Committee:

-Workshop on RFID Security (Asia, 2009 onward)

References

By request only.

Selected Publications (2008/09)

Journal publications:

1. Pedro Peris-Lopez, **Tieyan Li**, Julio C. Hernandez-Castro, Lightweight Props on the Weak Security of EPC Class-1 Generation-2 Standard, IEICE, Vol. E93-D, No.3, pp.-, Mar. 2010.
2. Pedro Peris-Lopez, **Tieyan Li**, Julio C. Hernandez-Castro, Juan M.E. Tapiador, “*Practical Attacks on a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard*”. Computer Communications (2009), Volume 32, Issues 7-10, 28 May 2009, Pages 1185-1193. doi: 10.1016/j.comcom.2009.03.010.
3. Tong Lee Lim, **Tieyan Li**, Sze Ling Yeo, “*A Cross-Layer Framework for Privacy Enhancement in RFID Systems*”. Pervasive and Mobile Computing, Elsevier Journal. Accepted in Sept. 2008.
4. **Tieyan Li**, Robert Deng, Guilin Wang, “*The Security and Improvement of an Ultra-lightweight RFID Authentication Protocol*”. International Journal of Security and Communication Networks, Wiley Publisher. Issue 2, 2008.
5. **Tieyan Li**, Guilin Wang, Robert Deng, “*Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols*”. Journal of Software, Academy publisher. Issue 3, 2008.

Book chapters:

1. **Tieyan Li**, Wei He, “*RFID Product Authentication in EPCglobal Network*”. Book Chapter in Development and Implementation of RFID Technology. To be published in 2009.
2. **Tieyan Li**, Tong-Lee Lim, “*RFID Anti-Counterfeiting: An Architectural Perspective*”. Book Chapter in RFID Security: Techniques, Protocols and System-On-Chip Design. To be published by Springer, 2008.
3. **Tieyan Li**, “*Flexible Multimedia Stream Authentication*”. Book Chapter in Handbook of Research on Secure Multimedia Distribution. To be published by IGI publisher, 2008.

Conference publications:

1. Shaoying Cai, **Tieyan Li**, Yingjiu Li, Robert Deng, Enabling Secure Secret Updating for Unidirectional Key Distribution in RFID-Enabled Supply Chains, The 11th International Conference on Information and Communications Security (ICICS'09), December 14-17, Beijing, China.
2. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. E. Tapiador, **Tieyan Li**, Jan C.A. van der Lubbe, “*Weaknesses in Two Recent Lightweight RFID Authentication Protocols*”, The 5th China International Conference on Information Security and Cryptology (Inscrypt'09). 12-15 Dec. 2009, Beijing, China.
3. Changshe Ma, Yingjiu Li, Robert Deng, **Tieyan Li**, “*RFID Privacy: Relation Between Two Notions, Minimal Condition, and Efficient Construction*”, ACM CCS 2009. November 9-13, 2009. Chicago, IL, USA.