# RAYLIN TSO

Department of Computer Science
National Chengchi University
64, Sec. 2, Zhi-nan Rd., Taipei 11605, Taiwan
Tel: +886-2- 2939-3091#62328
Fax: +886-2-2234-1409
E-mail: raylin@cs.nccu.edu.tw or tsoraylin@gmail.com

## EDUCATION:

04/2004 – 03/2006 University of Tsukuba, Tsukuba, Ibaraki, Japan
- *Ph.D.* in Risk Engineering, Graduate School of Systems and Information Engineering

04/2002 – 03/2004 University of Tsukuba, Tsukuba, Ibaraki, Japan
- *M.S.* in Risk Engineering, Graduate School of Systems and Information Engineering

04/1999 – 03/2002 University of Tsukuba, Tsukuba, Ibaraki, Japan
- *M.S.* in Master of Arts in Management Science – Division of Management and Public Policy

10/1991 –0 6/1995 National Tsing Hua University, Hsinchu, Taiwan
- *B.S.* in Industrial Engineering

## PROFESSIONAL and ACADEMIC EXPERIENCE:

**Dept. of Computer Science, National Chengchi University, Taiwan**
*Assistant Professor* *2/2008 – present*

**Graduate School of Systems and Information Engineering, University of Tsukuba, Japan**
*Academic researcher* *4/2006 – 1/2008*

## RESEARCH INTERESTS:

*Cryptography, Network Security, Information Security*

## HONORS and AWARDS

04/2006 *IPSJ Digital Courier* Funai Young Researcher Encouragement *Award*
(The Funai Foundation for Information Technology)

03/2006 Award for the best doctoral research in the Graduate School of Systems and Information Engineering, University of Tsukuba, Japan

## PUBLICATIONS:

### Refereed Journal Papers

1. **Raylin Tso**, "Signcryption revisited: security analysis and improvement schemes", Journal of Scientific & Practical Computing, Vol. 2, No.2, 2008.

2. **Raylin Tso**, Ying Miao, and Eiji Okamoto, "On algorithms for searching a consistent set of shares in a threshold scheme and the related covering problem", The Journal of Combinatorial Mathematics and Combinatorial Computing, Vol. 60, pp. 47-63, 2007.

3. **Raylin Tso**, Ying Miao, Takeshi Okamoto, and Eiji Okamoto, "How to verify the threshold *t* of the Shamir's (*t*,*n*)-threshold scheme", Transactions of Information Processing Society of Japan, Vol. 46(8), pp. 1824-1833, 2005.

4. **Raylin Tso**, Ying Miao, Takeshi Okamoto, and Eiji Okamoto, "A share-correctable protocol for the Shamir threshold scheme and its application to participant enrollment", Transactions of Information Processing Society of Japan, Vol. 46(8), pp. 1880-1888, 2005.

### Refereed Conference Papers

1. **Raylin Tso**, Yuan-Shun Chen, Li-Wei Chen, and Sheng-Shan Chan, "Security analysis and improvement of e-voting system based on oblivious signature", in the Proceedings of 2009 national Computer Symposium (NCS2009) Taiwan, to appear (in Chinese).

2. **Raylin Tso**, Sheng-Shan Chan, Li-Wei Chen, and Yuan-Shun Chen, "Certificateless signatures with message recovery", in the Proceedings of 2009 national Computer Symposium (NCS2009) Taiwan, to appear (in Chinese).

3. **Raylin Tso**, Li-Wei Chen, Yuan-Shun Chen, and Sheng-Shan Chan, "Certificateless proxy signature and its extension", in the Proceedings of 2009 national Computer Symposium (NCS2009) Taiwan, to appear (in Chinese).

4. **Raylin Tso**, Pei-Yin Wu, Lin-Wei Huang, and Wan-Chun Chuang, "Online fair games based on oblivious signatures", in the Proceedings of 2009 national Computer Symposium (NCS2009) Taiwan, to appear (in Chinese).

5. **Raylin Tso**, Takeshi Okamoto, and Eiji Okamoto, "Efficient short signatures from pairing", in Proceedings of the 6th International Conference on Information Technology: New Generations, IEEE Computer Society, pp. 417—422, 2009.

6. Atsushi Koide, **Raylin Tso**, and Eiji Okamoto, "A sanitizing signature scheme with indexing" in Proceedings of EUC 2008, pp.16-21, 2008.

7. Atsushi Koide, **Raylin Tso**, and Eiji Okamoto, "Convertible undeniable partially blind signature from bilinear pairings" in Proceedings of EUC 2008, pp.77-82, 2008.

8. **Raylin Tso**, "Signcryption scheme with standardized verification algorithm" in Proceedings of 2008 IEEE Aisa-Pacific Services Computing Conference, pp.1369-1374, 2008.

9. Atsushi Koide, **Raylin Tso**, Takeshi Okamoto and Eiji Okamoto, "A restricted undeniable designated verifier signature" in Proceedings of 2008 IEEE Aisa-Pacific Services Computing Conference, pp.1375-1380, 2008.

10. **Raylin Tso**, Xun Yi, and Xinyi Huang, "Efficient and short certificateless signature", in Proceedings of the 7th International Conference on Cryptology and Network Security, Springer, Lecture Notes in Computer Science, Vol. 5339, pp.64-79, 2008.

11. **Raylin Tso**, Xun Yi, Takeshi Okamoto, and Eiji Okamoto, "Efficient convertible limited verifier signatures", in Proceedings of the IEEE International Symposium on Information Theory (ISIT2008), IEEE Computer Society, pp.230-234, 2008.

12. **Raylin Tso**, Takeshi Okamoto, and Eiji Okamoto, '1-out-of-n oblivious signatures', in Proceedings of the 4th Information Security Practice and Experience

Conference (ISPEC2008), Springer, Lecture Notes in Computer Science, Vol. 4991, pp.45-55, 2008.

13. **Raylin Tso**, Juanma Gonzalez Nieto, Takeshi Okamoto, Colin Boyd, and Eiji Okamoto, "Verifier-key-flexible universal designated-verifier signatures", in Proceedings of the Eleventh International Conference on Cryptography and Coding (IMA2007), Springer, Lecture Notes in Computer Science, Vol. 4887, pp. 403-421, 2007.

14. **Raylin Tso**, Chunxiang Gu, Takeshi Okamoto, and Eiji Okamoto, "Efficient ID-based digital signatures with message recovery", in Proceedings of the 6th International Conference on Cryptology and Network Security (CANS2007), Springer, Lecture Notes in Computer Science, Vol. 4856, pp. 47-59, 2007.

15. **Raylin Tso**, Xun Yi, and Eiji Okamoto, "ID-based key agreement for dynamic peer groups in mobile computing environments", in Proceedings of the 2007 IEEE Asia-Pacific Services Computing Conference (IEEE APSCC 2007), pp103-110, 2007.

16. **Raylin Tso**, Takeshi Okamoto, and Eiji Okamoto, "ECDSA-verifiable Signcryption scheme with signature verification on the Signcrypted message", in Proceedings of the 3rd SKLOIS Conference on Information Security and Cryptology (INSCRYPT 2007), Springer, Lecture Notes in Computer Science, to appear.

17. **Raylin Tso**, Takeshi Okamoto, and Eiji Okamoto, "An improved signcryption scheme and its variation", in Proceedings of the IEEE International Conference on Information Technology (ITNG2007), pp. 772—778, 2007.

18. **Raylin Tso**, Takeshi Okamoto, and Eiji Okamoto, "Practical strong designated verifier signature schemes based on double discrete logarithms", in Proceedings of the SKLOIS Conference on Information Security and Cryptology (CISC2005), Lecture Notes in Computer Science, Vol. 3822, pp. 113--127, 2005.

19. **Raylin Tso**, Takeshi Okamoto, Tsuyoshi Takagi, and Eiji Okamoto, “An ID–based non–interactive tripartite key agreement protocol with *k*-resilience”, in Proceedings of The 3rd IASTED International Conference on Communications and Computer Networks (CCN 2005), pp. 38--42, 2005.

20. Takeshi Okamoto, **Raylin Tso**, and Eiji Okamoto, “One-way and two-party authenticated ID-based key agreement protocols using pairing”, Modeling Decisions for Artificial Intelligence (MDAI 2005), Lecture Notes in Artificial Intelligence, Vol.3558, pp. 122-133, 2005.

21. Takeshi Okamoto, **Raylin Tso**, Tsuyoshi Takagi, and Eiji Okamoto, “k-Resilient ID–based key distribution schemes from pairing-three party case”, in Proceedings of the Workshop on Coding and Cryptography 2005 (WCC2005), pp. 402-412, 2005.

22. **Raylin Tso**, Ying Miao, and Eiji Okamoto, “A new algorithm for searching a consistent set of shares in a threshold scheme with cheaters”, in Proceedings of the Information Security and Cryptology Conference (ICISC 2003), Lecture Notes in Computer Science, Vol.2971, pp377–-385, 2003.