＊邱錫彥副教授

所有發表期刊論文及研討會論文

1. Journal paper

(1) International Journal

[1] Wen-Tsai Ko, **Shin-Yan Chiou***, Erl-Huei Lu, and Henry Ker-Chang Chang, "Modifying the ECC-Based Grouping-Proof RFID System to Increase Inpatient Medication Safety," Journal of Medical Systems, Vol. 38, Issue 7, 12 pages, July., 2014. doi:10.1007/s10916-014-0066-5 (SCI) (Rank: 36/83, HEALTH CARE SCIENCES & SERVICES)

[2] **Shin-Yan Chiou** and Yi-Cheng Chen, "A Mobile, Dynamic and Privacy-Preserving Matching System for Car and Taxi Pools," Mathematical Problems in Engineering, Vol. 2014, Article ID. 579031, 10 pages, Mar., 2014.doi:10.1155/2014/579031. (SCI&EI) (Rank:23/90,ENGINEERING, MULTIDISCIPLINARY)

[3] **Shin-Yan Chiou** and Chi-Shiu Luo, "An Authenticated Privacy-Preserving Mobile Matchmaking Protocol based on Social Connections with Friendship Ownership," Mathematical Problems in Engineering, Vol. 2014, Article ID. 637985, 12 pages, Feb, 2014. doi:10.1155/2014/637985 (SCI&EI) (Rank: 23/90, ENGINEERING, MULTIDISCIPLINARY)

[4] **Shin-Yan Chiou** and Yao-Hsien Huang, "Mobile common friends discovery with friendship ownership and replay-attack resistance," Wireless Networks (WiNet), Vol. 19, Issue 8, pp. 1839-1850, Nov. 2013. doi:10.1007/s11276-013-0577-x (SCI&EI) (Rank: 45/78, TELECOMMUNICATIONS)

[5] **Shin-Yan Chiou**, "A Secure Cloud Storage System with Privacy, Integrity and Authentication," ICIC-ELB: ICIC Express Letters, Part B: Applications, Vol. 5 No. 3, pp. 843-849, June. 2014. (EI)

[6] **Shin-Yan Chiou**, "Authenticated Blind Issuing of Symmetric Key for Mobile Access Control System Without Trusted Parties," Mathematical Problems in Engineering, vol. 2013, Article ID. 858579, 11 pages, June, 2013. doi:10.1155/2013/858579 (SCI&EI)(Rank: 23/90, ENGINEERING, MULTIDISCIPLINARY)

[7] **Shin-Yan Chiou**, "Secure Method for Biometric-Based Recognition with Integrated Cryptographic Functions," BioMed Research International, vol. 2013, Article ID 623815, 12 pages, May, 2013.doi:10.1155/2013/623815 (SCI) (Rank: 50/160, BIOTECHNOLOGY & APPLIED MICROBIOLOGY)

[8] **Shin-Yan Chiou**, "An Exploration of the WiMAX Security Sublayer based on IEEE 802.16e-2005,"JDCTA: International Journal of Digital Content Technology and its Applications, Vol. 7, No. 9, pp. 57 ~ 65, May, 2013. (EI)

[9] **Shin-Yan Chiou**, "Trusted Online Transaction Methods Achieving Privacy and Fairness," AISS:Advances in Information Sciences and Service Sciences, Vol. 5 No. 5, pp. 370-377, March, 2013. (EI)

[10] **Shin-Yan Chiou**, "Mobile Common Friends Recognition with Privacy and Authenticity," ICIC-ELB: ICIC Express Letters, Part B: Applications, Vol. 4 No. 1, pp. 197-203, Feb. 2013. (EI)

[11] **Shin-Yan Chiou** and Yi-Xuan He,"Remarks on new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem," International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue 9, pp. 3322 - 3324, Sep, 2013.

[12] Wen-Tsai Ko, **Shin-Yan Chiou**, Erl-Huei Lu and Henry Ker-Chang, "A Privacy-Preserving Grouping Proof Protocol Based on ECC with Untraceability for RFID," AM: Applied Mathematics, Vol. 3 No. 4, pp. 336-341, April 2012.

[13] **S.Y. Chiou** and C.S. Laih, "On the Implementation of (2, n) Audio Cryptography Schemes without Computing Devices," International Journal of Electrical Engineering, Vol.11, No.1, pp. 53-58, Feb., 2004. (EI)

[14] C.S. Laih and **S.Y. Chiou**, "Cryptanalysis of An Optimized Protocol for Mobile Network Authentication and Security," Information Processing Letters, Vol. 85, Issue 6, pp. 339 - 341, March 2003. (EI, SCI)

[15] **S.Y. Chiou** and C.S. Laih, "A Tempo-Based t-out-of-n Audio Cryptography Scheme," IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E86-A, No.8, pp.2091-2098, Aug. 2003. (EI, SCI)

[16] **S.Y. Chiou** and C.S. Laih, “An Efficient Algorithm for Computing the LUC Chain,” IEE Proceedings-Computers and Digital Techniques, Vol.147, No.4, pp.263-265, July 2000. (EI, SCI)

(2) Domestic Journal

[1] **邱錫彥**、石俊彬, “一種兼顧隱私與公平的網路交易系統”，電腦與通訊(ICL Technical Journal), Vol. 127, March, 2009.

[2] **邱錫彥**、陳彥學, “可整合密碼技術之生物特徵處理方法”，電腦與通訊(ICL Technical Journal), Vol. 123, pp. 124-129, March, 2008.

[3] **邱錫彥**、陳彥學、王瑞堂、劉家蓁, “IEEE 802.16e-2005 WiMAX 安全子層初探”，電腦與通訊(ICL Technical Journal), Vol. 119, pp. 104-111, March, 2007.

2. Conference Papers:

(1) International Conference

[1] **Shin-Yan Chiou**, “A Secure Cloud Peer-to-Peer Storage System achieving Data Secrecy and Load Balance,” 2014 International Conference on Information, Business and Education Technology (ICIBET 2014), pp. 29 – 33, Beijing , China, Feb. 27-28, 2014.

[2] **Shin-Yan Chiou**, Jiun-Ming Chen, “An Electronic Voting Protocol Based on t–out–of–n Oblivious Signature Scheme,” International Conference on Business and Information 2013 (BAI 2013), pp. D263 – D274, Bali, Indonesia, July 7-9, 2013.

[3] **Shin-Yan Chiou**, "An Exploration of the WiMAX Security Sublayer based on IEEE 802.16e-2005,” International Conference on Business and Information 2013 (BAI 2013), pp. D48 – D57, Bali, Indonesia, July 7-9, 2013.

[4] Wen-Tsai Ko, Erl-Huei Lu, **Shin-Yan Chiou** and Henry Ker-Chang Chang, “A Mobile RFID-based Mutual Authentication Protocol using Elliptic Curve Cryptography for Security Patrolling Application,” RFIDsec 2012 Asia

Workshop, Taipei, Taiwan, Nov., 2012. pp. 63 – 71, Cryptology and Information Security Series, DOI 10.3233/978-1-61499-143-4-63.

[5] **Shin-Yan Chiou**, "A Secure Cloud Saving System With Privacy, Integrity and Authenticity," International Conference on Business and Information 2012 (BAI 2012), Sapporo, Japan, July 7-9, 2012.

[6] Wen-Tsai Ko, **Shin-Yan Chiou**, Erl-Huei Lu and Henry Ker-Chang, "An Improvement of Privacy-Preserving ECC-Based Grouping Proof for RFID," Proceeding of the 14th Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC2011) (ISBN: 978-1-4244-9790-4), pp. 1062-1064, Harbin, China, July 26-30, 2011. (IEEE) (EI) (http://www.csqrwc2011.org/default.php) (All papers will be indexed by EI Compendex and ISI Proceeding(ISTP).)

[7] C.N. Yang, C.C. Wu, C.Y. Chiu, **Shin-Yan Chiou**, and W.C. Liao, "Micropayment Schemes with Ability to Return Changes," Proceeding of the 11th International Conference on Information Integration and Web-based Applications & Services (iiWAS2009) (ISBN: 978-1-60558-660-1), pp. 354-361, Kuala Lumpur, Malaysia, Dec. 14-16, 2009. (BEST PAPER) (NSC 98-2219-E-006-001)

[8] **S.Y. Chiou**, S.Y. Chang and H.M. Sun, "Common Friends Divcovery with Privacy and Authentication," Proceedings of IEEE Conference on IAS2009 (Fifth International Conference on Information Assurance and Security), pp. 337-340, Xi'an, China, 2009.

[9] **S.Y. Chiou**, S.Y. Chang, Ghita Mezzour, Adrian Perrig and H.M. Sun, "A Trustable Reputation Scheme Based on Private Relationships," Proceedings of IEEE Conference on SNONAM2009 (The 2009 International Conference on Advances in Social Networks Analysis and Mining), pp. 19-24, Athens, Greece, 2009.

[10] **S.Y. Chiou** and J.B. Shi, "Web Transaction Methods Achieving Privacy and Fairness," International Conference on Business and Information 2009 (BAI 2009), Kuala Lumpur, Malaysia, July, 2009.

[11] H.M. Sun, **S.Y. Chang**, Y.H. Lin and S.Y. Chiou, "Efficient Authentication Schemes for Handover in Mobile WiMAX," Proceedings of IEEE Conference on ISDA 2008 (Eighth International Conference on Intelligent Systems Design and Applications), pp. 235 – 240, Dec., 2008.

[12] **S.Y. Chiou**, "Symmetric key generation using particular user keys," International Conference on Business and Information 2008 (BAI 2008), Seoul, July, Korea, 2008.

[13] **S.Y. Chiou**, "A Secure File Storage System," International Conference on Business and Information 2007 (BAI 2007), Tokyo, Japan, July, 2007.

[14] **S.Y. Chiou** and C.S. Laih, "Cryptanalysis of the RSA-based Fail-Stop Signature Schemes from IWSEC '99," The Second International Workshop for Asian Public Key Infrastructures, pp. 104-107, 2002.

[15] **S.Y. Chiou** and C.S. Laih, "An Easy Method to Implement Audio Cryptography Schemes without Computing Devices", Presented at the Rump Session, ASIA-CRYPT'01, Australia, 2001.

(2) Domestic Conference

[1]**邱錫彥**、王宗儒、陳俊名, "1-out-of-*n* Proxy Oblivious Signature Schemes and its e-voting Application," 第二十四屆資訊安全會議 (Cryptology and Information Security Conference 2014 (CISC 2014)), 國立政治大學, 台灣台北, May, 2014. (榮獲「第 24 屆資訊安全會議」論文佳作)

[2]**邱錫彥**、何懿軒、王宗儒, "基於 RSA 密碼系統之高效率 n 選 t 代理模糊簽章協定應用於公平線上博弈系統," 第二十四屆資訊安全會議(Cryptology and Information Security Conference 2014 (CISC 2014)), 國立政治大學, 台灣台北, May, 2014.

[3]**邱錫彥**、林嘉駿, "達到版本控管之版權管理系統," 2013 安全管理與工程技術國際研討會, 吳鳳科技大學, 台灣嘉義, Nov., 2013.

[4]**邱錫彥**、陳奕誠, “達到隱私性的行動共乘配對系統,” **第 11 屆台塑關係企業應用技術研討會**, 長庚大學, 台灣桃園, June, 2013.

[5]**邱錫彥**、賀榆辰, “具完整性、隱密性及部分檔名搜尋功能的安全 P2P 雲端檔案儲存系統,” 第二十三屆資訊安全會議(Cryptology and Information Security Conference 2013 (CISC 2013)), 南台科技大學, 台灣台南, May, 2013. (榮獲「第 23 屆資訊安全會議」最佳論文獎之佳作)

[6]**邱錫彥**、陳俊名, “基於模糊簽章之可多選電子投票系統,” 2012 全國電信研討會 (2012 National Symposium on Telecommunications (NST 2012)), 彰化師範大學, 台灣彰化, (Chuanghua), Nov. 16-17, 2012.

[7]**邱錫彥**、羅啟修,“利用社交網路達到行動任務匹配之系統與實作,” 第二十二屆資訊安全會議(Cryptology and Information Security Conference 2012 (CISC 2012)), 中興大學, 台灣台中(Taichung), May 30-31, 2012.

[8]**邱錫彥**、黃耀賢,“達到隱私性與認證性的行動社交網路交集探索系統與實作,” 第二十一屆資訊安全會議 (Cryptology and Information Security Conference 2011 (CISC 2011)), 虎尾科技大學, 台灣雲林, pp.322 - 327, May, 2011.

[9] **邱錫彥**、黃乙軒、黃繼元, “金鑰交換系統在 Windows Mobile 手機平台之實作,” 第九屆現代通訊科技應用學術研討會(CCA 2011), 北台灣科學技術學院, 台灣台北, pp. 1-6, March, 2011.

[10]**邱錫彥**、陳彥學,“基於 PKI 技術之生物辨識方法”，第十八屆資訊安全會議(Cryptology and Information Security Conference 2008, CISC 2008), pp. 377-389, May, 2008.

[11]**邱錫彥**, “平衡式的個人檔案安全儲存系統”，2006 年資訊管理暨電子商務經營管理研討會(Conference on 2006 Information Management and Electronic Commerce Business Management), pp. 42-42, Dec., 2006.

[12]**邱錫彥**、宋振華、林之寅, “具隱密性及完整性的個人檔案網狀儲存系統”，2006 電子商務與數位生活研討會(EC2006), Feb., 2006.

[13]賴溪松、**邱錫彥**, “Cryptanalysis of An Optimized Protocol for Mobile Network Authentication and Security,”第十二屆全國資訊安全會議(Proceedings of the Twelfth National Conference on Information Security), pp. 253-256, 2002.

[14]**邱錫彥**、賴溪松, “A Tempo-Based t-out-of-n Audio Cryptography Scheme,”第十一屆全國資訊安全會議(Proceedings of the Eleventh National Conference on Information Security), pp. 149-159, 2001. (Best Paper Award.)

[15]**邱錫彥**、賴溪松, “An Efficient Algorithm for computing Luc Chain,” 第十屆全國資訊安全會議(Proceedings of the Tenth National Conference on Information Security), pp. 34-39, 2000.