Name:	**Yau Wei Chuen**
Current Position:	Associate Professor
Address:	B1 # 108E, Xiamen University Malaysia, Jalan Sunsuria, Bandar Sunsuria, 43900 Sepang, Selangor
Programme:	Computer Science Technology, Digital Media Technology, Software Engineering
Tel:	03 8800 6803
E-mail:	wcyau@xmu.edu.my

EDUCATIONAL BACKGROUND

- Bachelor Degree, Department of Electrical Engineering, National Cheng Kung University, Taiwan, China (1999)
- Master Degree, Department of Electrical Engineering, National Cheng Kung University, Taiwan, China (2001)
- Ph. D Degree, Faculty of Engineering, Multimedia University, Malaysia (2013)

RESEARCH EXPERIENCE

- Research Fellow, Telekom Research and Development Sdn Bhd (TM R&D) (Jan 2016 - Mar 2016)
- MSC Malaysia Innovation Voucher Programme (2012)
- MDeC Researcher-Industry Attachment Program (2010-2011)
- Visiting Researcher, Eafit University, Colombia (Nov 2009)
- Project Leader / member for numerous research projects funded by government / industry.

RESEARCH INTERESTS

Cryptography, security protocols, intrusion detection, network security and privacy.

HONORS AND AWARDS

- Chartered Engineer (CEng)
- Certified Information Systems Security Professional (CISSP)
- GIAC Mobile Device Security Analyst (GMOB)
- GIAC Security Essentials (GSEC)
- Huawei Certified Network Associate - Constructing Basic Security Network (HCNA-Security)
- International Invention, Innovation and Technology Exhibition (ITEX) - Silver Medal, 2015
- Honorary member of the Phi Tau Phi Scholastic Honor Society, June 2001

- Research Creativity Award, 1999

ACADEMIC EXPERIENCE

Associate Professor, Xiamen University Malaysia (2016 – Present)
Lecturer / Senior Lecturer, Faculty of Engineering, Multimedia University (2004 - 2016)

REPRESENTATIVE PUBLICATIONS

- R. C.-W. Phan, **W.-C. Yau**, B.–M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)", *Information Sciences*, 178(13), pp. 2849-2856, 2008.
- **W.-C Yau**, Raphael C.-W. Phan, S.-H. Heng, B.-M. Goi, "Proxy re-encryption with keyword search: New definitions and algorithms with proofs", *International Journal of Security and Its Applications*, 5(2), pp. 75–90, 2011.
- **W.-C. Yau**, S.-H. Heng, S.-Y. Tan, Raphael C.-W. Phan, B.-M. Goi, "Efficient Encryption with Keyword Search in Mobile Networks", *Security and Communication Networks*, 5(12), pp. 1412 – 1422, 2012.
- **W.-C. Yau**, Raphael C. -W. Phan, S.-H. Heng, B.-M. Goi, "Security Models for Delegated Keyword Searching within Encrypted Contents", *Journal of Internet Services and Applications*, 3(2), pp. 233-241 2012.
- **W.-C. Yau**, Raphael C. -W. Phan, S.-H. Heng, B.-M. Goi, "Keyword Guessing Attacks on Secure Searchable Public Key Encryption Schemes with a Designated Tester", *International Journal of Computer Mathematics*, 90(12), pp. 2581-2587, 2013.
- **W.-C. Yau**, Raphael C. -W. Phan, "Security Analysis of a Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems", *Journal of Medical Systems*, 37 (6), DOI:10.1007/s10916-013-9993-9, 2013.
- **W.-C. Yau**, Raphael C. -W. Phan, "Cryptanalysis of a Chaotic Map-based Password-authenticated Key Agreement Protocol using Smart Cards", *Nonlinear Dynamics*, 79 (2), pp. 809-821, 2014.
- S.-Y. Tan, **W.-C. Yau**, B.-H. Lim, "An Implementation of Enhanced Public Key Infrastructure", *Multimedia Tools and Applications*, 74(16), pp. 6481-6495, 2015.
- L. Guo, **W.-C. Yau**, "Efficient Secure-Channel Free Public Key Encryption with Keyword Search for EMRs in Cloud Storage", *Journal of Medical Systems*, 39 (2), DOI: 10.1007/s10916-014-0178-y, 2015.
- W.-S Yap, R. C.-W. Phan, **W.-C. Yau**, S.-H. Heng, "Cryptanalysis of a New Image Alternate Encryption Algorithm Based on Chaotic Map", *Nonlinear Dynamics*, 80(3), pp. 1483-1491, 2015.
- M.I. Salam, **W.-C. Yau**, J.-J. Chin, S.-H. Heng, H.-C. Ling, R. C.-W. Phan, G.-S. Poh, "Implementation of Searchable Symmetric Encryption for Privacy-preserving Keyword Search on Cloud Storage", *Human-centric Computing and Information Sciences*, DOI:10.1186/s13673-015-0039-9, 2015.
- W.-S. Yap, R. C.-W Phan, B.-M. Goi, **W.-C. Yau**, S.-H. Heng, "On the Effective Subkey Space of Some Image Encryption Algorithms Using External Key", *Journal of Visual Communication and Image Representation*, 40, Part A, pp. 51-57, 2016.
- G. S. Poh, J.-J. Chin, **W.-C. Yau**, K.-K. R. Choo and M. S. Mohamad, "Searchable Symmetric Encryption: Designs and Challenges", ACM Computing Surveys (Accepted 2017).
- J. M. Hou, Y. L. Cheng, P. D. Chen, **W. C. Yau**, and C. S. Laih, "The Design and Implementation of a Distributed Network Intrusion Detection System with the Reconnaissance Ability", *Proceedings of Taiwan Area Network Conference*, Oct. 2000.

- J. M. Hou, **W. C. Yau**, and C. S. Laih, "Building an Intelligent Intrusion Detection System with Neural Network Approach," *IEEE Student Conference on Research and Development (SCOReD 2001)*, Feb. 2001.
- Y. S. Loh, **W. C. Yau**, C.T. Wong and W. C. Ho, "Design and Implementation of an XML Firewall", *Proceedings of the 2006 International Conference on Computational Intelligence and Security (CIS 2006)*, Guangzhou, China, Nov. 3-6, 2006, pp. 1147-1150.
- V. L. Chee, **W. C. Yau**, "Security Analysis of TORA Routing Protocol", *International Conference on Computational Science and its Applications (ICCSA 2007)*, Lecture Notes in Computer Science, vol. 4706, pp. 975-986, Springer-Verlag, 2007.
- **W.-C. Yau**, S.-H. Heng, B.-M. Goi, "Off-Line Keyword Guessing Attacks on Recent Public Key Encryption with Keyword Search Schemes", *The 5th International Conference on Autonomic and Trusted Computing (ATC 2008)*, Lecture Notes in Computer Science, vol. 5060, pp. 100-105, Springer-Verlag, 2008.
- Raphael C.-W. Phan, **W.-C. Yau**, B.-M. Goi, "Analysis of Two Pairing-based Three-party Password Authenticated Key Exchange Protocols", *3rd International Conference on Network and System Security (NSS 2009)*, pp. 102-106, 2009.
- **W.-C Yau**, Raphael C.-W. Phan, S.-H. Heng, B.-M. Goi, "Proxy Re-encryption with Keyword Search: New Definitions and Algorithms", *SecTech/DRBC*, Communications in Computer and Information Science, vol. 122, pp. 149–160, Springer Berlin Heidelberg, 2010.
- **W.-C Yau**, Raphael C.-W. Phan, B.-M. Goi, S.-H. Heng, "Cryptanalysis of a Provably Secure Cross-Realm Client-to-Client Password Authenticated Key Agreement Protocol of CANS '09", *The 10th International Conference on Cryptography and Network Security, (CANS 2011),* Lecture Notes in Computer Science, vol. 7092, pp. 172-184, Springer-Verlag, 2011.
- Y.-L. Er, **W.-C. Yau**, S.-Y. Tan, B.-M. Goi, "Email Encryption System Using Certificateless Public Key Encryption Scheme", *Information Technology Convergence, Secure and Trust Computing, and Data Management (ITCS & STA 2012)*, Lecture Notes in Electrical Engineering, vol. 180, pp. 179–186, Springer, 2012.
- D.A. Rahman, S.-H. Heng, **W.-C. Yau**, S.-Y. Tan, "Implementation of a Conditional Searchable Encryption System for Data Storage", *Computer Science and its Applications: Ubiquitous Information Technologies*, Lecture Notes in Electrical Engineering, vol. 330, pp. 469-474, Springer Berlin Heidelberg, 2015.
- S.-Y. Tan, J.-J. Chin, G.-S. Poh, Y. H. S. Kam, **W.-C. Yau**, "A Client-Server Prototype of a Symmetric Key Searchable Encryption Scheme Using Open-Source Applications," *The 5th International Conference on IT Convergence and Security (ICITCS 2015)*, Kuala Lumpur, pp. 1-5, IEEE, 2015.