Name:	**Iftekhar Salam**
Current Position:	Assistant Professor
Office	A4 # 407
Programme:	Information and Communication Technology
Tel:	03 8705 5121
E-mail:	Iftekhar.salam@xmu.edu.my

RESEARCH INTERESTS

Information security, cryptography, cryptanalysis, authenticated encryption, stream ciphers

EDUCATIONAL BACKGROUND

- *Bachelor Degree (Electronics Engineering Majoring in Telecommunication), Faculty of Engineering, Multimedia University, Malaysia (2008)*
- *Master Degree (Information Security), Department of Ubiquitous IT, Dongseo University, South Korea (2011)*
- *Ph. D Degree (Information Security), Science and Engineering Faculty, Queensland University of Technology, Australia (2018)*

WORKING EXPERIENCE

- Assistant Professor, Department of Information and Communication Technology, Xiamen University Malaysia, Malaysia (2018 to Present)
- Postgraduate Researcher, School of Electrical Engineering and Computer Science, Queensland University of Technology, Australia (2014 - 2018)
- Sessional Academic, Science and Engineering Faculty, Queensland University of Technology, Australia (2015 - 2017)
- Research Officer, Faculty of Engineering, Multimedia University, Malaysia (2013 - 2014)
- Member of Engineering Staff, Broadcasting and Telecommunications Convergence Future Technology Research Department, Electronics and Telecommunications Research Institute, South Korea (2011 - 2012)
- Research Associate, BK21 Project, Dongseo University, South Korea (2009 - 2011)
- Research Officer, Faculty of Engineering, Multimedia University, Malaysia (2008 - 2009)

HONORS/AWARDS/GRANTS

- Awarded QUTPRA, QUT Top Up Scholarship and QUT HDR Tuition Fee scholarship for pursuing PhD degree at Queensland University of Technology, Australia.
- Completed a training in Foundations of Learning and Teaching organised by the QUT Academic Development, Australia.
- Completed e-Grad School LEAP Module in Project Management.
- Awarded full time scholarship under the Brain Korea 21 (BK21) project for pursuing Master Degree at Dongeso University, South Korea.
- Participated 6 times in the Cross-Cultural Awareness Programme, organised by the Korean National Commission for UNESCO in co-operation with the ministry of Education, Science and Technology of the Republic of Korea.

REPRESENTATIVE PUBLICATION

- Iftekhar Salam, Leonie Simpson, Harry Bartlett, Ed Dawson, Kenneth Koon-Ho Wong, Fault Attacks on MORUS, Cryptography 2 (1), 2018.
- Md Iftekhar Salam, Wei-Chuen Yau, Ji-Jian Chin, Swee-Huay Heng, Huo-Chong Ling, Raphael CW Phan, Geong Sen Poh, Syh-Yuan Tan, Wun-She Yap, Implementation of Searchable Symmetric Encryption for Privacy-Preserving Keyword Search on Cloud Storage, Human-centric Computing and Information Sciences, Vol 5, Issue 1, pp. 1-16, 2015.
- Md Iftekhar Salam, Hoon Jae Lee, Algebraic Countermeasure to Enhance the Improved Summation Generator with 2-Bit Memory, Journal of Networks, Vol 8, No 5 (2013), pp. 977-984, 2013.
- Md Ifterkhar Salam, Hoon-Jae Lee, On the Algebraic Attack against Summation Type Keystream Generators, Int. Journal of Information and Computer Security, 2012 Vol.5, No.2, pp.132 – 149, 2012.
- Md Iftekhar Salam, Hoon-Jae Lee, Algebraic analysis of Shrinking Generator, Int. Journal of Math. Analysis, Vol. 6, 2012, no 50, pp. 2493-2499, 2012.
- Iftekhar Salam, Hassan Al Mahri, Leonie Simpson, Harry Bartlett, Ed Dawson, Kenneth Koon-Ho Wong, Fault Attacks on Tiaoxin-346, In Proceedings of the Australasian Computer Science Week Multiconference (ACSW 2018), ACM, 2018.
- Iftekhar Salam, Leonie Simpson, Harry Bartlett, Ed Dawson, Josef Pieprzyk, Kenneth Koon-Ho Wong, Investigating Cube Attacks on the Authenticated Encryption Stream Cipher MORUS, In Proceedings of the 16th IEEE Trustcom/BigDataSE/ICESS, IEEE Computer Society, 2017.
- Md Iftekhar Salam, Harry Bartlett, Ed Dawson, Josef Pieprzyk, Leonie Simpson, Kenneth Koon-Ho Wong, Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN, In Batten L., Li G. (eds), Applications and Techniques in Information Security (ATIS 2016), Vol 651, pp. 15-26, Springer, 2016.
- Md Iftekhar Salam, Kenneth Koon-Ho Wong, Harry Bartlett, Leonie Simpson, Ed Dawson, Josef Pieprzyk, Finding State Collisions in the Authenticated Encryption Stream Cipher ACORN, In Proceedings of the Australasian Computer Science Week Multiconference (ACSW 2016), ACM, 2016.
- Md Iftekhar Salam, Hoon Jae Lee, Algebraic Countermeasure to Enhance the Improved Summation Generator with 2-Bit Memory, IACR Cryptology ePrint Archive 2012: 282 (2012) .

- Md Iftekhar Salam, Madhusudan Singh, Sang Gon Lee, HoonJae Lee, Secure and Efficient Key Management Scheme for Wireless Mesh Network, The 35th Conference of the Korea Information Processing Society, pp. 844-847, Jeju Island, Korea, May 2011.
- Md Iftekhar Salam, Hoon-Jae Lee, A Review on the PKC-Based Security Architecture for Wireless Sensor Networks, Fifth International Conference on Computer Sciences and Convergence Information Technology, pp. 649-652, December 2010.
- Pardeep Kumar, Md Iftekhar Salam, Ahmed Galib Reza, Hyo Taek Lim, Hoon-Jae Lee, Performance Analysis of PingPong-128 Keystream Generator for Wireless Sensor Network, Fifth International Conference on Computer Sciences and Convergence Information Technology, pp. 653-658, December 2010.
- Md Iftekhar Salam, Pardeep Kumar, Hoon-Jae Lee, An Efficient Key Pre-distribution Scheme for Wireless Sensor Networks Using Public Key Cryptography, 6th International Conference on Networked Computing and Advanced Information Management, pp. 402-407, Seoul, Korea, August, 2010.
- Pardeep Kumar, Md Iftekhar Salam, SangGon Lee, HoonJae Lee, Addressing Secure Data Routing Scheme for Heterogeneous Sensor Network, 6th International Conference on Networked Computing and Advanced Information Management, pp. 86-90, Seoul, Korea, August, 2010.