Ali Abdulaziz Alhamdan
Assistant Professor, Computer Eng., CCIS, MU

Education

Ph.D. Cryptology, Electrical Engineering and Computer Science School, Queensland University of Technology (QUT), Australia, 2014.
M.I.T. Master of Information Technology, Queensland University of Technology (QUT), Australia, 2009.
B.Sc. Electrical Engineering, King Saud University (KSU), Saudi Arabia, 1997.

Academic Experience

March 2017 - Present: Assistant Professo r, College of Computer and Information Science, Majmaah University, Saudi Arabia.

Non-Academic Experience:

March 2014 - March 2017: GM, General Department of Security Controls and Governance, NIC, Saudi Arabia.
Jan. 2009 - Feb. 2010: Security Specialist, NIC, Saudi Arabia.
Jun 2003 - Jan. 2006: Data Center Engineer, NIC, Saudi Arabia.
Apr. 2002 - Jun 2003: Network Engineer, WAN Department, NIC, Saudi Arabia.
Oct. 1997 - Apr. 2002: Communication Engineer, Communication Department, NIC, Saudi Arabia.

Awards and Certificates

- **COBIT 5 Foundation**, APMG International, Riyadh, 2016.
- **Lean Six Sigma, Green Belt**, Riyadh, 2015.
- **Lead Implementer: ISO/IEC 27001:2013**, BSI, UK, 2014.
- **Graduation Certificate in Computer Networks**, Faculty of Information Technology, Queensland University of Technology (QUT), Brisbane, Australia, 2009.
- **Graduation Certificate in Information Security**, Faculty of Information Technology, Queensland University of Technology (QUT), Brisbane, Australia, 2009.

Publications

- Alhamdan, A. Real Implementation Issues in Symmetric Ciphers., The First Summit on Countering Cyber Crimes, Naif Arab University for Security Sciences (NAUSS), Riyadh, KSA, 2015.
- Alhamdan, A., Bartlett, H., Simpson, L., Dawson, E., and Wong, K. Flaws in the initialisation process of stream ciphers. In N. J. Daras and M.Th. Rassias, editors, Computation, Cryptography, and Network Security, pages 19-49. Springer International Publishing, 2015.
- Bartlett, H., Alhamdan, A., Simpson, L., Dawson, E., and Wong, K. Weaknesses in the initialisation process of the Common Scrambling Algorithm Stream Cipher. In Winterhof, A. and Schmidt, K. editors, Proc. Sequences and Their Applications (SETA 2014) 8th International Conference, Lecture Notes in Computer Science, Springer-Verlag, Melbourne, VIC, pages 220-233, 2014.
- Alhamdan, A., Bartlett, H., Dawson, E., Simpson, L. and Wong, K. Weak key-IV pairs in the A5/1 stream cipher. In Parampalli, U. and Welch, I. editors, Proc. 12th Australasian Information Security Conference (AISC 2014), Auckland, New Zealand}, Volume 149 of Conferences in Research and

Practice in Information Technology (CRPIT), pages 23-36. Australian Computer Society, Inc., 2014.

- Teo, S., Bartlett, H., Alhamdan, A., Simpson, S., Wong, K. and Dawson, E. State convergence in bit-based stream ciphers. Cryptology ePrint Archive, Report 2013/096, 2013. http://eprint.iacr.org/.
- Alhamdan, A., Bartlett, H., Dawson, E., Simpson, L. and Wong, K. Slid pairs in the initialisation of the A5/1 stream cipher. In Thomborson, C. and Parampalli, U., editors, Proc. 11th Australasian Information Security Conference (AISC 2013), Adelaide, Australian}, volume 138 of Conference in Research and Practice in Information Technology (CRPIT), pages 3-12. Australian Computer Society, Inc., 2013.
- Alhamdan, A., Bartlett, H., Simpson, L., Dawson, E., and Wong, K. State convergence in the initialisation of the Sfinks stream cipher. In Pieprzyk, J. and Thomborson, C., editors, Proc. 10th
- Australasian Information Security Conference (AISC 2012), Melbourne, Australia}, volume 125 of Conference in Research and Practice in Information Technology (CRPIT), pages 27-32. Australian Computer Society, Inc., 2012.
- Alhamdan, A., Bartlett, H., Dawson, E., Simpson, L. and Wong, K. Slide Attacks on the Sfinks Stream Cipher. Proc. 6th International Conference on Signal Processing and Communication Systems, IEEE, Radisson Resort, Gold Coast, QLD, Dec. 2012.
- Teo, S., Alhamdan, A., Bartlett, H., Simpson, L., Wong, K. and Dawson, E. State convergence in the initialisation of stream ciphers. In Parampalli, U. and Hawkes, P., editors, {\em Proc. 16th Australasian Conference Information Security and Privacy, (ACISP 2011), Melbourne, Australia}, volume 6812 of {\em Lecture Notes in Computer Science (LNCS)}, pages 75-88. Springer, 2011.