Dr. Liaqat Ali Khan

Email: liaquatalikhan@gmail.com

ACADEMIC AND PROFESSIONAL INTERESTS

- Cryptology
- Computer and Network Security
- Speech Communication

EDUCATION

Ph.D in Information Security (2011)
College of Signals
National University of Sciences & Technology
Rawalpindi, Pakistan
Dissertation: Analysing Encrypted Speech

B. Eng. in Avionics (1992)
College of Aeronautical Engineering, Risalpur
Project: PC Controlled Digital Exchange
Graduation Date : December, 1992.

EXPERIENCE

- 1993-1998 : Technical Officer, Electronic and Telecommunication Equipment Maintenance Organization, Pakistan.

- 1998-2000 : Research Officer, Communication Research and Development Organization, Pakistan.

- 2000-2003 : Instructor, College of Aeronautical Engineering, Rislapur Pakistan.

- 2009 onwards : Director Cyber Warfare / Cryptology Centre, Research and Development Organization, Pakistan. Adjunct Faculty IAA, Air University.

AWARDS

- Quaid-e-Azam Medal for 4th Position in HSSC Exam Rawalpindi Board

- NUST Endowment and Mega IT Fund Scholarship for Indigenous PhD
- IRSIP Scholarship for Concordia University Canada
- Best Student Paper Award International Conference on Computer Science and Applications, San Francisco, USA, 24-26 Oct, 2007.
- Tamgha-e-Imtiaz (2015)

PUBLICATIONS

1. **L. A. Khan** & M.S Baig, "Reconstructing a Class of Cipher Systems used in Wireless Digital Communications." Proceedings of the IEEE International Conference on Electrical Engineering, Lahore, Pakistan, 11-12 April, 2007.

2. **L. A. Khan**, M. S. Baig & M. Ashraf, "Exploiting Silence for Ciphertext Only reconstruction of Stream Ciphered Digitized Voice." The 2007 International Conference on Security and Management (SAM'07), Las Vegas, Nevada, USA, 25-28 June, 2007.

3. **L. A. Khan** & M. S. Baig. "Cryptanalysis of Keystream Reuse in Stream Ciphered Digitized Speech using HMM based ASR Techniques." International Conference on Computer Science and Applications, San Francisco, USA, 24-26 Oct, 2007. (Best Student Paper Award)

4. M. Ashraf, M.S. Baig, **L .A. Khan** & Ali Hassan, "Parallel Implementation of 2D-DWT by Purging Read After Write Dependency for High Speed Applications." Proceedings of the IEEE Conference on Emerging Technologies (ICET 2007), Islamabad, Pakistan, 13-14 Nov, 2007.

5. **L. A. Khan** & M. S. Baig. "Automated Cryptanalysis of Plaintext XORs of Waveform Encoded Speech." IAENG International Journal of Computer Science, Volume 35 Issue 2, pp 234-241, May, 2008.

6. **L. A. Khan** & M. S. Baig. "A Hidden Markov Model Based Speech Recognition Approach to Automated Cryptanalysis of Two Time Pads." Advances in Computational Algorithms and Data Analysis, Lecture Notes in Electrical Engineering, Volume 14, pp 159-168, Springer, September, 2008

7. **L. A. Khan** & M. S. Baig. "A Server Based ASR Approach to Automated Cryptanalysis of Two Time Pads in Case of Speech." Proceedings of the International Conference on Information Assurance and Security (IAS'08), pp 103-107, Naples, Italy, September, 2008.

8. **L. A. Khan**, M. S. Baig and Ali Hassan. "Cryptanalysis of Stream Enciphered Speech Communication in a Keystream Reuse Situation." Mehran University Research Journal of Engineering & Technology, Vol. 29, No. 1, pp 61-78, Jan, 2010.

9. Farkhund Iqbal, **L. A. Khan**, B. Fung, M. Debabi. "Email Authorship Verification for Forensic Investigation." Proceedings of the 2010 ACM Symposium on Applied Computing (SAC), pp 1591-1598, Sierre Switzerland, March, 2010.

10. **L. A. Khan**, M. S. Baig & Amr M. Youssef. "Speaker Recognition from Encrypted VoIP Conversations." Digital Investigation Vol. 7, No. 1-2, pp 65-73, Oct, 2010.

11. **L. A. Khan**, F. Iqbal, M.S. Baig. "Speaker Verification from Partially Encrypted Compressed Speech for Forensic Investigation." Digital Investigation Vol. 7, No. 1-2, pp 74-80, Oct, 2010.

12. **L. A. Khan**, M. S. Baig & Ali Hassan. "Cryptanalysis of Two Time Pads in Case of Compressed Speech." Computers and Electrical Engineering, Vol. 37 No. 4, pp 559-569, Jul, 2011.

13. Usama Ahmed, Ammar Masood, **L. A. Khan**. "Quantifying the Role of Access Control in End to End Network Security." The 2011 International Conference on Security and Management (SAM'11), Las Vegas, Nevada, USA, 18-21 July, 2011.

14. Naila M. Abbassi, M. S. Baig, **L. A. Khan**. "Improved Trust based Key Management for End to End Secure Communication in Cellular Netwroks." 8th International Conference on Security of Information and Networks, Sochi, Russia, 8-10 Sep, 2015.