HELWAN
UNIVERSITY

Maged Hamada Ibrahim (B.Sc., M.Sc., PhD)

(Associate Professor)

Curriculum Vitae @ 2015

mhii72@gmail.com
Mobile: (+20) 100-203-9091

Maged Hamada Ibrahim (BSc, MSc, PhD)
(Associate Professor)

Contact Information

Department of Electronics,
Communications & Computers,
Faculty of Engineering,
Helwan University,
Helwan, Cairo, Egypt

HELWAN UNIVERSITY

E-mail:
mhii72@gmail.com

Phone: +20-100 2039091

Home address:
5, Hassan El-Kadi St.,
El-Haram, Giza; Egypt.

Education

Research Scholar (Post Ph.D.)
Department of Computer Science & Eng. (CSE building)
University of Connecticut,
Connecticut, Storrs, USA,
2008.

Doctorate of Philosophy (Ph.D.)
Department of Electronics, Communications & Computers,
Faculty of Engineering, Helwan University,
Cairo, Egypt,
2005.

Master of Science (M.SC.)
Department of Electronics, Communications & Computers,
Faculty of Engineering, Helwan University,
Cairo, Egypt,
2001.

Bachelor of Science (B.SC.)
Communications and Computers Engineering,
Faculty of Engineering, Helwan University,
Cairo, Egypt,
1995.

Main Research Interests

Engineering Cryptography, Communications and Network Security:
More specifically, working on the design of efficient cryptographic and non-cryptographic security solutions to communication systems, Networking and transmission protocols. Very much interested in secure distributed multiparty computations and public-key cryptography. Other things that interest me are number theory and the inspection of mathematics for designing secure communication and network security systems. I'm also interested in digital human rights and secure electronic government.

Professional Career Experience

Graduate Student
1995
Department of Electronics, Communications and Computers,
Faculty of Engineering, Helwan University,
Cairo, Egypt.

Stood the first in my class with the honor degree (Excellent).
Project grad: Excellent

Demonstrator (Tutorial Assistant)
1996-2001
Department of Electronics, Communications and Computers,
Faculty of Engineering, Helwan University,

Cairo, Egypt.

Assisted in teaching classical communications, Digital communications, spread spectrum communication theory, electromagnetics and transmission lines, basics of antennae engineering, probabilities and stochastic processes, advanced communication engineering and communication systems.

Lecturer Assistant
2001-2005
Department of Electronics, Communications and Computers,
Faculty of Engineering, Helwan University,
Cairo, Egypt.

Assisted in Teaching academic education courses for undergraduates, the courses include:

- Cryptography and Network Security.
- Information and Coding Theory.
- Probabilities and Random processes.
- Estimation Theory and the Theory of Classical Detection.
- Radar Systems.
- Satellite Communication Systems
- Wireless Communications and Wireless Security.
- Electromagnetic propagation and EM security.
- Signal Analysis and Linear systems.
- Analog and Digital Communication Systems.
- Data Communication and Networking.
- Principles of Microprocessors, Machine and Assembly Language.

Professional Career Experience (cont.)

Assistant Professor
2006-2012
Department of Electronics, Communications and Computers,
Faculty of Engineering,
Helwan University,
Cairo, Egypt.

Associate Professor
2013-present
Department of Electronics, Communications and Computers,
Faculty of Engineering,
Helwan University,
Cairo, Egypt.

Experienced in teaching the following courses and subjects:

- Continuous wave, Analog and Digital Communication Systems.
- Noise in communication systems.
- Cryptography and Network Security.
- Information and Coding Theory.
- Probabilities, Random and Stochastic processes.
- Estimation Theory and the Theory of Classical Detection.
- Radar Systems.
- Satellite Communication Systems
- RF Optimization, Wireless Communications and Wireless Security.
- Spread spectrum and code division multiple access.
- Electromagnetic propagation and EM security.
- Signal Analysis and Systems.
- Data Communication and Networking.
- Logic Circuits Design.
- Digital signal processing.

Professional Career Experience (cont.)

Other administrative, academic, and cultural Activities:

- Project proposal referee at the **National Telecommunications Regulatory Authority (NTRA)**, 2012.
- Project proposal referee at the **National Telecommunications Regulatory Authority (NTRA)**, 2013.
- Member of the steering committee of the **1st International conference on electrical and computer system engineering (MSA university, Cairo Egypt)** http://msaee.com/Conference-Committees.php
- Joined the consultant team for constructing the enterprise network of Helwan University Specially the part concerning the internet connectivity security modulus and equipment (e.g. Firewalls, Proxies, Pixs, antivirus, etc.)
- Joined the consultant team for constructing the Measurements, Microwave and Communications Labs at the International Academy of Engineering and Media Science.
- Chair for the curriculum committee at MSA University, Cairo, Egypt.
- Chair of the research committee at MSA University, Cairo, Egypt.
- Expert/consultant at the International Academy of Engineering and Media Science, Faculty of Media Engineering, Cairo, Egypt. (Fall 2011).
- Reviewer in several international journals: Elsevier, International Journal of Network Security, Springer Verlag, Cryptologia, many other American, European and Asian Journals.

Research Scholar

Departement of Computer Science & Engineering (CSE building),
University of Connecticut,
Connecticut, Storrs, USA,
2008.

- **Research scholar activity**: In the field of cryptography and communications security, more precisely, in secure multiparty computations, adaptive security, deniable encryption and secure function evaluation.
- **Period**: One academic year.
- **Advisors:**
  Prof. Aggelos Kiayias (CSE University of Connecticut)
  Prof. M. Moti Yung (Google Inc., University of Colombia)

Ph.D. Study

- **Ph.D.** Department of Electronics, Communications and Computers, Faculty of Engineering, Helwan University, Cairo, Egypt, 2005.
- **Dissertation:** Secret Sharing Schemes: Theory and Analysis.
- **Advisors:** Prof. A. H. El-Sawy and Prof. I. I. Ibrahim.
- **Thesis Context:** Developing fast, efficient and secure multiparty computation protocols for the sharing of the RSA function. Introducing novel methods for secure fully distributed and robust threshold digital signature schemes with honest majority.
- **Publications extracted from the PhD thesis:**
  - M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Robust Threshold Elliptic Curve Digital Signature, in proceedings of the IEEE 46th symposium on Circuits and Systems, Cairo, Egypt, 2003.
  - M. H. Ibrahim, I. I. Ibrahim, A. H. El-Sawy, Fast Three-Party Shared Generation of RSA Keys without Distributed Primality Tests, in proceedings of Information Systems: New Generation Conference (ISNG 2004), Las Vegas, Nevada, USA, pp. 5-10, 2004.

Ph.D. Study (Cont.)

  - M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Fast Fully Distributed and Threshold RSA Function Sharing, in proceedings of Information Systems: New Generation Conference (ISNG 2004), Las Vegas, Nevada, USA, 2004, pp. 11-15.

- M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Reducing the Risk of the Honest Dealer Assumption in Robust Threshold RSA Function Sharing, in proceedings of the 1st International Computer Engineering Conference on New Technologies for the Information Society (ICENCO 2004), Cairo, Egypt, 2004.
- M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Fully Distributed and Robust Threshold RSA Function Sharing Efficient for Small Number of Players, (extended), chapter 11 in Nadia Nedjah, Luiza de Macedo (eds.), Embedded Cryptographic Hardware, Methodologies and Architectures, Nova-Science Publishers, New York, USA, 2004, ISBN: 1-59454-012-8.

M.Sc. Study

- **M.Sc.** Department of Electronics, Communications and Computers, Faculty of Engineering, Helwan University, Cairo, Egypt, 2001.
- **Thesis:** Network Security Systems (Analysis of Symmetric Cryptosystems)
- **Advisors:** Prof. A. H. El-Sawy and Prof. I. A. Ali.
- **Thesis Context:** Analyzing multiple encryptions (e.g. Triple DES, DESX) and multiple encryption multiple modes of the block ciphers for their strength against exhaustive key search attacks (brute force attacks). Introducing novel secure ideas to get rid of the redundancy in the input key length to be equal to the effective key length without a significant increase in hardware and encryption time.
- **Publications extracted from the MSc thesis:**
  - Analysis of triple encryption schemes as a block cipher protection against exhaustive key search, Journal of engineering and applied science, vol.3, June 2001.
  - Multiple encryption modes with optimal secret parameters, Journal of engineering and applied science, 2001.

Publications

Single-Author Publications:

1. M. H. Ibrahim, AATCT: Anonymously Authenticated Transmission on the Cloud with Traceability, ***International Journal of Advanced computer science and applications (IJACSA)***, 6(9),pp. 251-259, October, 2015

2. M. H. Ibrahim, Secure Anonymously Authenticated and Traceable Enterprise DRM System, ***International Journal of Computer Applications*** 126(3):1-9, September 2015. Published by Foundation of Computer Science (FCS), NY, USA.

3. M. H. Ibrahim, Efficient Robust and Secure E-DRM with Encrypted Content Search, ***International Journal on Information (Information-Tokyo)***, Vol. 18, No. 6(A), pp. 2531-2546, Tokyo-Japan, 2015.

4. M. H. Ibrahim, Secure and Robust Digital Rights Management Protocol with Efficient Storage, ***International Journal on Information (Information-Tokyo)***, Vol. 18, No. 2, pp.625-640, Tokyo-Japan, 2015.

5. M. H. Ibrahim, Realizing Sender's Deniability in Public Key Encryption via Random Coins Isolation", in ***European Journal of Scientific Research***, Vol. 119, Issue 2, 2014.

6. M. H. Ibrahim, Efficient Coercion Resistant Public Key Encryption, ***International Journal of Computer Science & Security (IJCSS)***, Vol. 8, Issue 1, 2014, pp. 1-13.

7. M. H. Ibrahim, "New Capabilities of visual cryptography", ***International journal of computer science issues (IJCSI)***, Vol. 9, Issue 5, No. 1, September 2012.

Publications (Cont.)

8. M. H. Ibrahim, A Novel Approach to Adaptively Secure Message Transmission in The Non-Erasure Model, ***International Journal of Advanced Research in Computer Science***, Vol. 2, No. 6, Nov-Dec 2011. (ICV Impact Factor = 5.47)

9. M. H. Ibrahim, Efficient Secret Handshaking Protocol, ***International Journal of Advanced Research in Computer Science***, Vol. 2, No. 6, Nov-Dec 2011. (ICV Impact Factor = 5.47)
10. M. H. Ibrahim, A novel approach to fully private and secure auction: A sealed-bid Knapsack auction, ***International Journal of Research and Reviews in Applied Science (IJRRAS)***, Vol. 9, Issue 2, Nov. 2011.

11. M. H. Ibrahim, Noninteractive, Anonymously Authenticated and Traceable Message Transmission for VANETs, in the ***International Journal of Vehicular Technology (IJVT), Hindawi publishing corporation***, 2009.

12. M. H. Ibrahim, Resisting Traitors in Linkable Democratic Group Signatures, ***International Journal of Network Security (IJNS)***, Vol. 9, No. 1, 2009, pp. 51-60.

13. M. H. Ibrahim, Receiver-Deniable Public-Key Encryption, ***International Journal of Network Security (IJNS)***, Vol.8, No.2, PP.159-165, 2009.

14. M. H. Ibrahim, A Method for Obtaining Deniable Public-Key Encryption , ***International Journal of Network Security (IJNS)***, Vol.8, No.1, PP.1-9, Jan. 2009.

15. M. H. Ibrahim, Efficient Dealer-Less Threshold Sharing of Standard RSA, ***International Journal of Network Security (IJNS)***, Vol.8, No.1, PP.134–145, Jan. 2009.

16. M. H. Ibrahim, Eliminating Quadratic Slowdown in Two-Prime RSA Function Sharing, ***International Journal of Network Security (IJNS),*** Vol. 7, No. 1, 2008, pp. 107-114 .

17. M. H. Ibrahim, Efficient Incoercible and Universally Verifiable Multi-authority Yes/No Voting Scheme, in proceedings of the ***6th International Conference on Informatics and Systems (INFOS)***, Cairo, Egypt, 2008.

18. M. H. Ibrahim, Two-Party private Vector Dominance: The All-Or-Nothing Deal, in proceedings of ***IEEE Information Technology: New Generations (ITNG 2006),*** Las Vegas, Nevada, USA, IEEE proceedings, pp. 166-171, 2006.

19. M. H. Ibrahim, Verifiable Threshold Sharing of a Large Secret Safe Prime, in proceedings of the ***IEEE International Conference on Information Technology Coding and Computing ITCC 2005 (1), Las Vegas, Nevada, USA***, pp. 608- 613, 2005.

Co-Authored Publications:

20. Ahmed H. Soliman, Maged H. Ibrahim, Salwa H. El-Ramly, Enhancing Efficiency of Enterprise Digital Rights Management, in proceedings of ***7th IEEE International Conference on Advanced Computer Science and Information Systems (ICACSIS), Indonisia, 2015.***

21. Ahmed H. Soliman, Maged H. Ibrahim, Adel E. El-Hennawy, Improving

Security and Efficiency of Enterprise Digital Rights Management, in proceedings of the ***6th IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT)***, Texas, USA, 2015.

22. Fatty M. Salem and Maged H. Ibrahim, Efficient PU Detection and Authentication Protocol for Secure Cognitive Spectrum Sharing in Hostile Environment***, International journal on information (information-Tokyo)***, Tokyo, Japan, Vol.17, No.9(B), September 2014, pp.4515-4525.

Publications (Cont.)

23. Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim" "Robust Asynchronous Authentication Protocol for Secure Cognitive Spectrum Sharing", in ***European Journal of Scientific Research***, Vol. 118, Issue 4, 2014.

24. Fatty M. Salem, Maged H. Ibrahim, Ihab A. Ali and I. I. Ibrahim, Matched-Filter-based Spectrum Sensing for Secure Cognitive Radio Network Communications. ***International Journal of Computer Applications (IJCA),*** 87(18), 2014, New York, USA, pp. 41-46.

25. Fatty M. Salem, Maged H. Ibrahim, and I. I. Ibrahim, "Energy Detection Based Sensing for Secure Cognitive Spectrum Sharing in the Presence of Primary User Emulation Attack," ***IEEK Transactions on Smart Processing and Computing,*** vol. 2, no. 6, 2013, IEIE SPC, Korea, pp. 357-366.

26. Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim, Secure Authentication Scheme Preventing Wormhole Attacks in Cognitive Radio Networks, ***Asian Journal of Computer Science and Information Technology***, Vol. 2, No. 04 (2012)

27. M. H. Ibrahim, A. Kiayias, M. Yung, H-S. Zhou, Secure Function Collection With Sublinear Storage, in proceedings of ***ICALP***-2009, ***Lecture Notes in Computer Science (LNCS), Springer Berlin/Heidelberg***, Vol. 5556, pp. 534-545, July 2009. (IF Impact Factor: 0.402).

28. Fatty M. Salem, Maged H. Ibrahim, and Ibrahim I. Ibrahim, Efficient Non-Interactive Secure Protocol Enforcing Privacy in Vehicle-to-Roadside Communication Networks, ***International Journal of Vehicular technology, Hindawi publishing corporation***, 2012.

29. Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim, A Primary User Authentication Scheme for Secure Cognitive TV Spectrum Sharing, ***IJCSI International Journal of Computer Science Issues,*** Vol. 9, Issue 4, No 2, July 2012***,*** IF = (0.242 self).

30. Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim, "Non-interactive Secure and Privacy Preserving Protocol for Inter-vehicle Communication Networks," ***ITNG***, pp.108-113, 2010 ***Seventh International Conference on Information Technology: New Generations***, ***Las Vegas, Nevada, USA***, 2010.

31. Fatty M. Salem, Maged H. Ibrahim, I. I. Ibrahim, "Non-interactive Authentication Scheme Providing Privacy among Drivers in Vehicle-to-Vehicle Networks," ***ICNS***, pp.156-161, 2010 ***Sixth International Conference on Networking and Services, Cancun, Mexico,*** 2010.

32. Ali M. Allam, Maged H. Ibrahim and Ibrahim I. Ibrahim, A New Key Establishment Approach for 3rd Generation Mobile Network with Signature Scheme, in proceedings of ***Fourth international computer***

engineering conference (ICENCO 2008), Cairo, Egypt.

33. I. I. Ibrahim, M. H. Ibrahim, A. M. Allam, A method for fast revocation of certificate-less public key cryptography, ***International Conference on Computer Engineering and Systems, ICCES'06***, pp. 250–253, 2006.

34. I. I. Ibrahim, M. H. Ibrahim, Ali M. Allam, An Efficient Key Management and Signcryption Scheme for Mobile Communication, ***IEEE International Conference on Research, Innovation, and Vision for Future***, pp. 217-220, 2008.

Publications (Cont.)

35. I.I. Ibrahim, M.H. Ibrahim, Ali M. Allam, A New Approach for Privacy in E-government, ***second annual Workshop on Information Security and Privacy (WISP)***, 2007.

36. Ibrahim I. Ibrahim Maged H. Ibrahim Ali M. Allam, A NEW KEY ESTABLISHMENT APPROACH FOR 3RD GENERATION MOBILE NETWORK, ***Journal of Engineering Sciences, Assiut University***, Vol. 36, No. 4, pp.877-886, July 2008.

37. M. H. Ibrahim, I. I. Ibrahim, A. H. El-Sawy, Fast Three-Party Shared Generation of RSA Keys without Distributed Primality Tests, in proceedings of ***Information Systems: New Generation Conference (ISNG 2004), Las Vegas, Nevada, USA***, pp. 5-10, 2004.

38. M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Fast Fully Distributed and Threshold RSA Function Sharing, in proceedings of ***Information Systems: New Generation Conference (ISNG 2004), Las Vegas, Nevada, USA***, 2004, pp. 11-15.

39. M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Reducing the Risk of the Honest Dealer Assumption in Robust Threshold RSA Function Sharing, in proceedings of the ***1st International Computer Engineering Conference on New Technologies for the Information Society (ICENCO 2004), Cairo, Egypt,*** 2004.

40. M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Robust Threshold Elliptic Curve Digital Signature, in proceedings of the ***IEEE 46th symposium on Circuits and Systems, Cairo, Egypt,*** 2003.

41. R. M. Sayed, Maged H. Ibrahim, , Z. B. Nossair, Group key exchange protocol for users with individual passwords, ***Journal of Engineering and Applied Science, Cairo, Egypt***, vol. 55, no. 4, pp. 327–342, 2008.

42. D. N. Shaban, M. H. Ibrahim, and Z. B. Nossair, "Enhanced Verifier-Based Password Authentication Key Agreement Protocol for Three-Parties", ***Journal of Engineering Science***, ***Assiut University***, vol. 36, No. 6, pp. 1513-1522 , November 2008.

43. B. Morgan, M. H. Ibrahim, and G. Abdelfadel, "Efficient Public Key Encryption with Keyword Search", ***Journal of Engineering Science, Assiut University***, vol. 38, No. 3, pp. 749-761, May 2010.

Publications (Cont.)

44. A. A. Rashad, M. H. Ibrahim and Z. B. Nossair," New secret key exchange based on recent cryptographic schemes", ***Mansoura Engineering Journal***, vol. 33, no. 3, September 2008, pp. E1-E10. Mansoura University, Cairo, Egypt.

45. B. Morgan, M. H. Ibrahim, and G. Abdelfadel, "Security Using the Efficient

Public Key Encryption with Keyword Search System", ***Journal of Engineering Science, Assiut University***, vol. 39, No. 3, pp. 607-624, May 2011.

46. Maged H. Ibrahim, I. A. Ali, A. H. El-Sawy, Multiple encryption - Multiple modes with optimal secret parameters, ***Journal of Engineering and Applied Science, Cairo, Egypt,*** vol. 49, no. 6, pp. 1177–1195, 2002.

47. Maged H. Ibrahim, I. A. Ali, A. H. El-Sawy, Analysis of triple encryption schemes as a block cipher protection against exhaustive-key search, ***Journal of Engineering and Applied Science, Cairo, Egypt,*** vol. 48, no. 3, pp. 491–507, 2001.

Book Chapters Publications

48. M. H. Ibrahim, Verifiable Threshold Sharing of a Large Secret Safe- Prime, Book Chapters (extended), ***chapter 9*** in Nadia Nedjah, Luiza de Macedo (eds.), ***New Trends in Cryptographic Systems***, Nova Science Publishers, New York, USA, 2006, ISBN: 1-59454-977-X.

49. M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, A. H. El-Sawy, Fully Distributed and Robust Threshold RSA Function Sharing Efficient for Small Number of Players, (extended), chapter 11 in Nadia Nedjah, Luiza de Macedo (eds.), ***Embedded Cryptographic Hardware, Methodologies and Architectures***, Nova-Science Publishers, New York, USA, 2004, ISBN: 1-59454-012-8.

Published Books

50. "Efficient and Secure Message Transmission in Vehicular Ad Hoc Networks", ***Lambert Academic Publishing (LAP)***, 2012.

51. "Coercion Resistant Cryptosystems", ***Lambert Academic Publishing (LAP)***, 2014.

MSc/PhD Supervision

Supervising 10+ MSc and PhD Dissertations. Seven have already granted the degree. Research Topics include:

- Secret key authentication and exchange.
- Authentication, Traceability, Anonymity and Privacy of VANETs
- Password authenticated key exchange.
- Public key infrastructures with advanced capabilities.
- Secure and efficient authentication in Vehicular Networks
- Cognitive Radio Networks: Spectrum detection and authentication
- Public key cryptosystems with keyword search.
- Security issues in digital rights management.
- Security issues in cloud computing

Special Skills

Some of which are:

- **Languages**: Excellent English.
- **Computer & Programming Skills:** Visual Basic, C/C++/C#, Java2 Standard edition (J2SE, JDK), Java2 enterprise (J2EE), Java DB, SQL, Html, XML, Tomcat Apache server (Sun Application Server), and basics of Oracle DB and Open-SSL.
- **Digital Design:** VHDL programing, FPGA Xilinx/Altera digital design suites.
- **Typesetting:** Advanced knowledge of the professional typesetting package LATEX and Microsoft Office
- **Editing:** Strong technical/scientific writing and grammar skills.

Date of Birth: 22/05/1972

Personal Data

Place of Birth: Dokki, Giza , Egypt.
Nationality: Egyptian.
Marital Status: Single.
Affiliations:

- **Associate Professor**, Department of Electronics, Communications and Computers, Faculty of Engineering, Helwan University.
- **Adjunct Associate Professor**, Department of Electrical Communications Engineering, October University of Modern Science and Arts (MSA), 6th October City, Cairo, Egypt.

References

- Prof. Abdel-Rahman El-Sawy (mob.020-1222109730) [Helwan University]
  Departement of Electronics, Communications and Computers,
  Faculty of Engineering, Helwan University
  Helwan University, Cairo-Egypt
  President of System Engineering of Egypt (SEE).

- Prof. El-Sayed Mustafa Saad (mob.020-1001243111) [Helwan University]
  Departement of Electronics, Communications and Computers,
  Faculty of Engineering, Helwan University
  Helwan University, Cairo-Egypt.

- Prof. Ibrahim Ismail Ibrahim (mob.020- 1001544331) [Helwan University]
  Departement of Electronics, Communications and Computers,
  Faculty of Engineering, Helwan University
  Helwan University, Cairo-Egypt

- Prof. Ihab Abdel Wahab Ali (mob.020-1005321124) [Helwan University]
  Departement of Electronics, Communications and Computers,
  Faculty of Engineering, Helwan University
  Helwan University, Cairo-Egypt

- Prof. Mohamed Ghazy [Effat University]
  Departement Head
  Faculty of Engineering
  Effat University
  Kingdom of Saudi Arabia.

- Prof. Aggelos Kayaias [University of Connecticut]
  Department of Computer Science and Engineering,
  University of Connecticut
  Connecticut, Storrs, USA.