

DR. LO'AI A. TAWALBEH^{1,2}

ASSOCIATE PROFESSOR OF COMPUTER ENGINEERING,
IEEE SENIOR MEMEBR.

¹COMPUTER ENGINEERING DEPARTMENT,
UMM AL-QURA UNIVERSITY;
P.O.BOX 715, MAKKAH, 21955, SAUDIA ARABIA

²DIRECTOR OF THE CRYPTOGRAPHIC HARDWARE AND INFORMATION
SECURITY LAB (CHIS),
[TENURE] AT COMPUTER ENGINEERING DEPARTMENT,
JORDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY,
P.O.BOX 3030, IRBID, 22110, JORDAN

E-MAIL 1: LATAWALBEH@UQU.EDU.SA
E-MAIL 2: tawalbeh@just.edu.jo
E-MAIL 3: Loai.tawalbeh@gmail.com
WEBSITE: www.just.edu.jo/~tawalbeh

PERSONAL INFORMAITON:

- **Date of Birth:** 1977
- **Citizenship:** Jordanian
- **Marital status:** Married with Four children

EDUCATIONAL QUALIFICATIONS:

October 2004

- **PhD** in Electrical and Computer Engineering from Oregon State University (OSU), Corvallis, Oregon, USA. **GPA= 4.00/4.00**. Main Supervisor: Prof. Cetin Kaya Koc.

Thesis Title: "A Novel Unified Algorithm and Hardware Architecture for Integrated Modular Division and Multiplication in GF(p) and GF(2n) Suitable for Public-Key Cryptography".
October 28, 2004.

October 2002

- **Master** of Science in Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon, USA. **GPA= 4.00/4.00**. Main Supervisor: Dr. Alexandre F. Tenca.

Thesis Title: "Radix-4 ASIC Design of a Scalable Montgomery Modular Multiplier Using Encoding Techniques". October 23, 2002.

June 2000

- **Bachelors of Science** in Electrical and Computer Engineering from Jordan University of Science and Technology (JUST), Jordan. GPA = Very Good.

Key Research Words: Cyber security, Cryptography, Mobile Cloud and Security, Efficient Software/Hardware implementations for Cryptographic Algorithms, Wireless Security, Modular Arithmetic, Elliptic Curve Cryptography, FPGA Design, Multimedia Security.

WORK EXPERIENCE

Sept. 2013- Present: Associate Visiting Professor at Computer Engineering Department,
Umm Al-Qura University, Saudi Arabia

- Teaching mainly Graduate course in the Master of Science (MSc) program in the track of information security. Those courses include: Computer forensics, information security, cryptography, and Cloud Computing Systems. Also, I am member in many committees such as the study plan committee, MS steering committee, and strategic planning committee.
- Conducting Research in cyber security and cloud computing management and security.
- Supervising three MSc students theses in different cyber security related topics.
- Writing research proposals and grants. Within 2 years I won 3 research grants with an approximate budget of 1.2 Million US Dollars.

Feb. 2005- Present: [Tenure] Associate Professor (March 2013-present), Assistant Professor (2005-2012), Computer Engineering Department, Jordan University of Science and Technology, Jordan

- Teaching graduate and undergraduate course in information and network security, cryptography, advanced arithmetic for cryptosystems design and Embedded systems design using FPGA's.
- Supervised 12 MSc students theses in cyber security related topics, and acting as examiner for another 10 MSc theses. For the undergraduate program, I supervised 13 senior graduation projects.
- In 2009, I won a research grant for distinguished professors in Jordan. I established the first research lab (Cryptographic Hardware and Information Security Lab) in the field of cryptography and information security which is the first cyber security research lab in Jordan and the region. I am the lab director till now.
- Prepare with my colleagues the study plans for the graduate/undergraduate programs in JUST.
- I served as member and chair in many committees at the department/college and university level.

April 2005- June 2012: Part-time Adjunct-Assistant Professor, New York Institute of Technology-Jordan's Campus (program offered from 2001 till 2013). <http://www.nyit.edu/jordan/>

- Teach and develop the curriculum of the courses in the graduate program (MSc program of information, computer and network security). Those courses include: Intrusion Detection, Computer forensics and Digital Evidence, Secure Software Engineering, Operating Systems Security, Information and Network Security, and Cryptography.

Sept. 2011- June 2013: Part-time Adjunct-Assistant/Associate Professor, Princess Sumaya University, Amman, Jordan

- Teach courses in the graduate program (MSc Program in Information Systems Security and Digital Criminology). Those courses included: Network Security, Digital forensics, and Cryptography.
- Supervised successfully three MSc students theses during the 2 years I worked there.

Feb. 2007- Feb. 2009: Part-time Adjunct-Assistant professor, Depaul University- Jordan's campus

- Teach courses in the MSc graduate program in wireless networking and security. Those courses included: Cellular and Wireless Communications, Voice and Data Integration, Wireless Systems Engineering and Deployment, Network Security.

GRANTS AND FUNDED RESEARCH PROJECTS

- 1- **(420,000 \$) December 2014. Principle Investigator (PI).** “New and Efficient Mobile Cloud Computing Model based on Cloudlet Concept for Intensive Computer Vision and RFID Applications”. Supported by NSTIP plan- King AbdulAziz City for Science and Technology (KACST), KSA.
- 2- **(313,300 \$) May 2014, Co-Investigator.** “ A Novel Framework for Secure Cryptosystems against Side Channel Attacks”. Supported by NSTIP plan- King AbdulAziz City for Science and Technology (KACST), KSA.
- 3- **(362,670 \$) October 2013. Principle-Investigator (PI),** “Promoting Energy as a First Class Metric in Network Simulations”. Supported by NSTIP plan-King AbdulAziz City for Science and Technology (KACST), KSA.
- 4- **(80,000 \$) June 2010, Principle Investigator,** “Efficient Cryptographic Processor for Internet and Wireless Security Based on Elliptic Curve Cryptography”. Ministry of High Education-Jordan.
- 5- **(300,000\$) Jan. 2002, CO-Investigator,** National Science Foundation (NSF) grant CCR-0093434- "Computer Arithmetic Algorithms and Scalable Hardware Designs for Cryptographic Applications", Research Assistant Scholarship, Oregon State University, USA, 2002-2004.
- 6- **(94,000\$) August 2001:** National Scholarship from Jordan Government to get Master and Doctoral degrees at Oregon State University, Corvallis, Oregon, USA, (August 2001-January 2005).

RESEARCH LABS AND ACTIVITIES:

1. Established the **Cryptographic Hardware and Information Security Lab (CHIS)** at Jordan University of Science and Technology (JUST), Jordan in 2010. (**The Director**). The lab aims to spread the knowledge and enhance the research in the area of cryptography and data security regionally and internationally.
2. Founding and Chairing the International Workshop on Mobile Cloud Computing systems, Management, and Security (MCSMS-2015). London, UK, June 2015.
3. Chairing the IEEE International Workshop on Software Defined Systems, AZ, USA, March 2015
4. Consultant for : Universal Research Solutions Inc., Missouri, USA: Feb 2012-Feb 2013.
5. Research Member at the Information Security Lab at Oregon State University, USA.
6. Research Member at the Machine Intelligence Research Lab, USA (started Jan. 2011-Present).
7. Establish an Incubator for a leading regional Software development company called I-HORIZON at Jordan University of Science and Technology to bridge the gap between industry and the academia, and give the students the hands on needed to involve them in the market and keep them updated with up to date technologies.
8. Coordinate and attend a MENTOR GRAPHICS training in: "FPGA Design and Verification Training Course". The training was attended by the engineers and faculty from computer Engineering Dept., 2011.
9. Founder of the ICICs conference in Amman, Jordan, Dec., 2009.
10. Coordinator of the Mentor Graphics Higher Education Program (HEP) at Jordan University of Science and Technology, 2007

MEMBERSHIP OF SCIENTIFIC AND PROFESSIONAL SOCIETIES

1. Senior IEEE member.
2. Jordan Engineering Association
3. AMAN-Jordanian association for family and society protection. This association is a Member at International Union for family management and protection. Among its goals is to protect family and women and youth from diseases such as AIDS, and from drugs.
4. Member of “Future Protectors”, which is an international group that aims to protect youth from AIDS and DRUGS worldwide.

SELECTED PUBLICATIONS: (24 Journals, 26 Conferences and 2 Book Chapters)

Journal Papers (24):

1. **Lo'ai A. Tawalbeh**, Fadi Ababneh, Yaser Jararweh, Fahd AlDosari. “Trust Delegation based Secure Mobile Cloud Computing Framework”. In the International Journal of Information and Computer Security, Accepted May 2016.
2. **Lo'ai A. Tawalbeh**, Anas Basalamah, Rashid Mehmood, and Hala Tawalbeh. “Greener and Smarter Phones for Future Cities: Characterizing the Impact of GPS Signal Strength on Power Consumption”. IEEE Access Journal. DOI (identifier) 10.1109/ACCESS.2016.2532745. March 2016.
3. **Lo'ai Tawalbeh**, Yousef Haddad, Omar Khamis, Elhadj Benkhelifa Yaser Jararweh, and Fahd AlDosari, “Efficient and Secure Software-Defined Mobile Cloud Computing Infrastructure”. International Journal of High Performance Computing and Networking (IJHPCN). Vol 9, No. 2, March 2016.
4. Elhadj Benkhelifa, Tom Welsh, **Lo'ai A. Tawalbeh**, Yaser Jararweh and Anas Basalamah. "Energy Optimization for Mobile Device Power Consumption: A Survey and a Unified View of Modeling for a Comprehensive Network Simulation". Submitted to the Mobile Networks and Applications journal (IF=1). December 2015.
5. **Lo'ai A. Tawalbeh**, Yaser Jararweh, Fadi ababneh and Fahd Dosari. Large Scale Cloudlets Deployment for Efficient Mobile Cloud Computing. **Journal of Networks**. Vol 10, No 1 (2015), 70-76, Feb 2015.
6. Yaser Jararweha, Huda Ababneh, Mohammad Alhammourib, **Lo'ai A. Tawalbeh**. “Energy Efficient Multi-Level Network Resources Management in Cloud Computing Data Centers”. Journal of Networks. Vol. 10, No. 5, May 2015.
7. Y. Jararweh, , O. Al-Sharqawi, N. Abdulla, **L. A. Tawalbeh**, M. Alhammouri High-Throughput Encryption for Cloud Computing Storage System. **International Journal of Cloud Applications and Computing**, IGI Global, USA, Vol 4 No 2, Sept. 2014.
8. **L. A. Tawalbeh**, M. Mowafi and W. Aljobi . "The Potential of using Elliptic Curve Cryptography for Multimedia Encryption". **IET Information Security Journal**, Institution of Engineering and Technology, Vol 7, No 2, pp.1-8, UK, June 2013.
9. O. Melhm, **L. A. Tawalbeh**, M. Mowafi and M. Batati." A More Secure Image Hiding Scheme using Pixel Adjustment and Genetic Algorithm”. **International Journal of Information Security and Privacy**, Vol 7, No. 3, pp.1-15, IGI Global, USA, Sept. 2013.

10. Y. Jararweh, **L. A. Tawalbeh**, H. Tawalbeh, and A. Moh'd." 28 Nanometers FPGAs Support for High Throughput and Low Power Cryptographic Applications". *Journal of Advances in Information Technology*, Vol 4, No 2, pp. 84-90, ACADEMY Publisher, Finland, May 2013.
11. **L. A. Tawalbeh**, O. BaniMelhem and M. Al-Batati. "A Novel High Quality High Capacity Image Hiding Scheme Based on Image Compression and Optical Pixel Adjustment Process". *Information Security Journal; A Global Perspective*. Vol. 21, Issue 5, pp.256-268. Taylor and Francis, USA. Aug 2012.
12. M. Mowafi, **L. A. Tawalbeh** Walid Aljobe and M. Alrousan." C3SM: Information Assurance Based on Cryptographic Checksum with Clustering Security Management Protocol. " *Journal of Information Security*. Vol 7, No.2, pp 272-280, Scientific Research Publisher, USA. October 2012
13. **L. A. Tawalbeh**, H. Al-Hajsalem, T. Abu Qtaish and A. Khatabeh and. "A New efficient symmetric encryption algorithm design and implementation". *Journal of Information Assurance and Security*, Vol 7, No.2, pp 101-109. Dynamic Publishers, Inc., USA , June 2012.
14. **L. A. Tawalbeh**, Y. Jararweh and A. Moh'md. "An Integrated Radix-4 Modular Divider/Multiplier Hardware Architecture for Cryptographic Applications". *The International Arab Journal of Information Technology*, Vol. 9, No. 3, pp 284-290, May 2012.
15. Y. Jararweh, **L. A. Tawalbeh**, H. Tawalbeh, and A. Moh'd. "Hardware Performance Evaluation of SHA-3 Candidate Algorithms". *Journal of Information Security*. Vol 3 No.2, pp 69-76, Scientific Research Publisher, USA. April 2012.
16. **L. A. Tawalbeh** and Q. Abu Al-Haija. "Enhanced FPGA Implementations for Doubling Oriented and Jacobi- Quartics Elliptic Curves Cryptography". *Journal of Information Assurance and Security*, Vol.6, Issue 3, pp. 167-175, Dynamic Publishers, Inc., USA. 2011.
17. **L. A. Tawalbeh**, A. Mohammad and A. A. Gutub. "Efficient FPGA Implementation of a Programmable Architecture for GF(p) Elliptic Curve Crypto Computations". *Journal of Signal Processing Systems*, Vol (59) No. (3), pp. 233-244. Springer, June 2010
18. Q. A. Al-Haija and **L. A. Tawalbeh**. "Efficient Algorithms and Architectures for Elliptic Curve Crypto-Processor Over GF (P) Using New Projective Coordinates Systems". *Journal of Information Assurance and Security*, Vol. 6, Issue 1, pp. 63-72. Dynamic Publishers, Inc., USA, January 2011.
19. **L. A. Tawalbeh** and Saedeh Swaidan." Hardware Design and Implementation of ElGamal Public-Key Cryptography Algorithm". *International Journal of Information Security; A global Perspective*, Vol (19) Issue 5, pp. 243-252, Taylor and Francis, October 2010.
20. F. Muhaya, Q. Alhaija and **L. A. Tawalbeh**. "Applying Hessian Curves in Parallel to improve Elliptic Curve Scalar Multiplication Hardware". *International Journal of Security and Its Applications*, pp. 27-38, Vol.4. No.2. SERSC (Science & Engineering Research Support Center). Korea. April 2010.
21. **L. A. Tawalbeh**, Saed Swedan, A. Gutub "Efficient Modular Squaring Algorithms for Hardware Implementation in GF(p)". *International Journal of Information Security; A global Perspective*, Vol (18) Issue 3, pages 131-138. Taylor and Francis. June 2009.

22. F. Tenca, S. Park and **L. A. Tawalbeh** “Carry-save representation is shift-unsafe: the problem and its solution”. *IEEE Transactions on Computers*, Vol 55, No 5 pp. 630-636, May 2006.
23. **L. A. Tawalbeh**, A. F. Tenca, and C. K. Koc. "A radix-4 scalable design". *IEEE Potentials Magazine*, vol. 24 No.2, pages 16-19, April/May 2005.
24. A. Tenca and **L. A. Tawalbeh** “An Algorithm for Unified Modular Division in GF(p) and GF(2ⁿ) Suitable for Cryptographic Hardware”. *IEE Electronics Letters*, 40(5),304-306, March 2004.

Conference Papers (26 papers):

1. **L o’ ai A. Tawalbeh**, Waseem Bakhader, Houbing Song. “A Mobile Cloud Computing Model Using the Cloudlet Scheme for Big Data Applications” 2015 IEEE Conference on Connected Health: Applications, Systems and and Engineering Technologies (CHASE 2016). To be held 27-29 June 2016 in Washington DC, USA.
2. Elhadj Benkhelifa, Thomas Welsh, **Lo’ ai A. Tawalbeh** and Yaser Jararweh, “Framework for Mobile Devices Analysis”. In the 7th Ambient systems and Networks conference (ANT 2016). *Procedia Computer Science*, (83), pp 1188-1193, DOI: [10.1016/j.procs.2016.04.246](https://doi.org/10.1016/j.procs.2016.04.246) Madrid, Spain, May 23-25, 2016.
3. Khadijah S. Bahwairath and **Lo’ ai A. Tawalbeh**, “Cooperative Models in Cloud Computing and Mobile Cloud Computing”. In the proceedings of the 23rd IEEE international conference of Telecommunications (ICT2016), Greece, May 16-18,2016. To appear.
4. Elhadj Benkhelifa, Thomas Welsh, **Lo’ ai A. Tawalbeh**, Fahd Al-Dosari, Abdallah Khreishah, and Yaser Jararweh, “GA-Based Resource Augmentation Negotiation for Energy-Optimised Mobile Ad-hoc Cloud”. In the proceedings of the 4th IEEE Mobile Cloud conference, Oxford, UK, March 28-31, 2016.
5. **Lo’ ai A. Tawalbeh**, Norah Alassaf, Waseem Bakheder, and Alaa Tawalbeh “Resilience Mobile Cloud Computing: Features, Applications and Challenges”. In the proceedings of the 2015 International Symposium on Web of Things and Big Data (WoTBD 2015), in conjunction with 5th IEEE eCONF, Bahrain,18-20 October 2015.
6. **Lo’ ai A. Tawalbeh**, R. Al-Qassas, N. Darwazeh, Y. Jararweh, and Fahd AlDosari, “ Secure and Efficient Cloud Computing Framework”. In the Proceedings of **the IEEE International Conference on Cloud and Autonomic computing (Cloud Cyber Security workshop)**, pp.291-295, **Cambridge, MA, USA**, Sept., 21-24, 2015. DOI: [10.1109/ICCAC.2015.45](https://doi.org/10.1109/ICCAC.2015.45).
7. Khadijah S. Bahwairath, **Lo’ ai A. Tawalbeh** and Anas Basalamah, “Efficient Techniques for Energy Optimization in Mobile Cloud Computing”. In the Proceedings of the **12th ACS/IEEE International Conference on Computer Systems and Applications-AICCSA, Workshop on Internet of Things, Systems, Management and Security (IoTSMS), Morocco, Nov. 17-20, 2015**.
8. M. Al-Ayyoub, Y. Jararweh, **Lo’ ai A. Tawalbeh**, E. Benkhelifa and A. Basalamah. “Power Optimization of Large Scale Mobile Cloud Computing Systems”. In the proceedings of the 9th International Symposium on Performance Modeling and Evaluation of Computer and Telecommunication Networks (PMECT 2015) of FiCloud-2015 (proceedings published by IEEE CPS)., **Rome, Italy**, 24-28 Aug. (2015).
9. **Lo’ ai A. Tawalbeh**, Fahd AlDosari , and Waseem Bakhader. “ Cloud Security: Challenges and Solutions”. In the Proceedings of the **3rd International IBM Cloud Academy Conference**, May 21-23, 2015, Budapest, Hungary.

10. E. Benkhelifa, Thomas Welsh, **Loai Tawalbeh**, Yaser Jararwehc and A. Basalamah, "User Profiling for Energy Optimization in Mobile Cloud Computing". In the 6th Ambient systems and Networks conference (ANT 2015). Procedia Computer Science 52 (2015) 1159 – 1165, UK, June 2015.
11. **Lo'ai Tawalbeh**, Nour S. Darwazeh, Raad S. Al-Qassas, and Fahd AIDosari, " A Secure Cloud Computing Model based on Data Classification". In the International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2015), held in conjunction with **the 6th ANT conference 2015**, Procedia Computer Science, Volume 52, 2015, Pages 1153–1158, UK. June 2015.
12. **Lo'ai Tawalbeh**, Yousef Haddad, Omar Khamis, Fahd AIDosari, and Elhadj Benkhelifa "Efficient Software-Based Mobile Cloud Computing Framework". In the IEEE international conference on Cloud Engineering (IC2E 2015), Arizona, USA, March 9-13-2015.
13. Y. Jararwah, **L. A. Tawalbeh**, F. Ababneh, Abdallah Khreishah and F. Dosari. " Scalable Cloudlet-based Mobile Computing Model". In The 11th International Conference on Mobile Systems and Pervasive Computing-Mobi-SPC 2014, ELSEVIER, Procedia Computer Science 34, pp.434 – 441, Niagara Falls, Canada, , August 17-20, 2014.
14. Y. Jararwah, **L. A. Tawalbeh**, F. Ababneh and F. Dosari, "Resource Efficient Mobile Computing using Cloudlet Infrastructures". In the Proc. of the IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), IEEE Xplore digital library, pp.373-377, China, December 11- 13, 2013.
15. A. Moh'd, Y. Jararweh and **L. A. Tawalbeh**. "AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation ". In the Proc. of the 7th IEEE International conference on Information Assurance and Security. IEEE Xplore digital library, pp.292-297, Malacca, Malaysia, Dec. 5-8, 2011.
16. Y. Jararweh, H. Tawalbeh, **L. A. Tawalbeh**, and A. Moh'd. "FPGA Performance Evaluation Of SHA-3 Candidate Algorithms". In the Proc. of the 5th Mosharaka International Conference on Communications, Networking and Information Technology -MIC-CNIT2011. Dubai , UAE, Dec. 16-18, 2011.
17. A. Moh'd, N. Aslam, H. Marzi and **L. A. Tawalbeh**. "Hardware Implementations of Secure Hashing Functions on FPGAs for WSNs". In the Third International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2010), Istanbul, Turkey. July 2010.
18. **L. A. Tawalbeh**, Wafaa Kanakri and Lina Ebbini." Efficient Random Number Generators (RNG) based on Nonlinear Feedback Shift Registers (NLFSR). In the International Conference on Information and Communication Systems (ICICS), Jordan, Dec.20-22, 2009.
19. **L. A. Tawalbeh**, M. Alrousan, and D. Alansari, "Survey of efficient public-key management schemes for wireless sensor networks" ICPCM 2009, Sydney- Australia. Dec. 12-14, 2009.

20. A. Moh'd, **L. A. Tawalbeh** and Amadou sowe. "A Novel Method to Guarantee QoS during DOS Attacks for IPTV using SIP. In the second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009). IEEE Xplore digital library, pp.838-842, London, UK. August 2009.
21. M. Alrousan, Khaled Al-Saleh and **L. A. Tawalbeh**, "Voice-Driven Smart Wheel Chair. In The Third AUS-International Symposium on Mechatronics. Sharjah, UAE, Sponsored by IEEE, April 18-20, 2006.
22. **L. A. Tawalbeh**, A. F. Tenca, S. Park, and C. K. Koc. "An efficient hardware architecture of a scalable elliptic curve crypto-processor over $GF(2^m)$ ". In the Advanced Signal Processing Algorithms, Architectures, and Implementations XV, Proceedings of SPIE Conference, F. T. Luk, editor, pages 216-226, Volume 5910, San Diego, California, USA, August 2-4, 2005.
23. A. Rjoub and **L. A. Tawalbeh**. "A Low Power, High Frequency and High Precision Multiplier Architecture in $GF(p)$ ". International e-Conference of Computer Science (IeCCS). Athens, Greece, May 19-31, 2005. Appeared in Lecture Series on Computer and Computational Sciences, Editor-in-Chief: T. Simos, ISSN:1573-4196, Volume (2), pp. 178-183, Brill Academic Publishers, Netherlands, 2005.
24. **L. A. Tawalbeh** and A. F. Tenca "An Algorithm and Hardware Architecture for Integrated Modular Division and Multiplication in $GF(p)$ and $GF(2^n)$ ". In the IEEE 15th International Conference on Application-specific Systems, Architectures and Processors (ASAP), Galveston, TX, USA, IEEE Press, pp.247-257, Sept. 2004.
25. **L. A. Tawalbeh**, A. F. Tenca, S. Park, and C. K. Koc. "A dual-field modular division algorithm and architecture for application specific hardware". Thirty-Eighth Asilomar Conference on Signals, Systems, and Computers, Pages 483-487, IEEE Press, Pacific Grove, California, USA, November 7-10, 2004.
26. A. F. Tenca and **L. A. Tawalbeh**. "An efficient and scalable radix-4 modular multiplier design using recoding techniques". Thirty-Seventh Asilomar Conference on Signals, Systems, and Computers, Pages: 1445-1450, vol.2 IEEE Press, Pacific Grove, California, USA, November 9-12, 2003.

Book Chapters:

1. **Lo'ai A. Tawalbeh**. "Ch 10: Lightweight crypto and security". Book title: Security and Privacy in Cyber-Physical Systems: Foundations and Applications (**Wiley Publisher**). Editors: Houbing Song, Glenn A. Fink, Sabina Jeschke, and Gilad L. Rosner. to appear 2016.
2. **Lo'ai A. Tawalbeh** and Cetin Kaya Koc, Book Chapter (Ch5): "Efficient elliptic curve cryptographic hardware design for wireless security". Book: Wireless Security and Cryptography. Editors: Sklavos Nicolas, Nicolas Zhang, ISBN: 084938771X, **Taylor & Francis Ltd., USA**, 2007

Citations (321, H-index=10):

<https://scholar.google.com/citations?user=gw17mOoAAAAJ&hl=en>

TRAINING AND CERTIFICATES

1. Nominated to teach the cryptography unit to the talented youth in MAWHEBA program (in cooperation with Johns Hopkins CENTER for TALENTED YOUTH, USA). Done in Summer 2015 (24th July-16th august).
2. EMC certified proven professional “ Cloud Infrastructure and Services: Cloud Architect track”. January 2015.
3. Attending the training workshop: “Accelerating Scientific Applications using GPUs”, KAUST, KSA, Sept.18th, 2013.
4. Coordinate and attend a MENTOR GRAPHICS training in: "FPGA Design and Verification Training Course". The training was attended by the engineers and faculty from computer Engineering Dept., 2011.
5. Attended Ethical Hacking Training workshop (CEH)- April 2009.
6. Specialized workshop on “Creativity and Innovation”. June 2006.
7. Training workshop on “Preparation the Leaders of Information Technology”, Feb. 2006.
8. Training workshop on “Testing and Evaluation (University Examination Methodologies)”.,July, 2005.
9. Java Certified Programmer, 2001

MASTER STUDENTS SUPERVISED:

1. **N. Darwazah**. A Reliable Confidentiality-based Cloud Storage Framework. Computer Engineering Department, MS Thesis, Princes Sumaya University, Jordan. Dec , 2013
2. **Y. Haddad**. **Lightweight Provable Data Possession Mobile Cloud Computing Framework**. Computer Engineering Department, MS Thesis, Princes Sumaya University, Jordan. Dec , 2013
3. **F. Ababneh**.**Secure Cloudlet-based Mobile Cloud Computing Model**. Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, **November 2012**.
4. **M. Abu Maghli**, “Design and Implement Secure Integrated Terminal Authentication Protocol in E-passport Inspection Systems ". Computer Engineering Department, MS Thesis, August, 2012.
5. **A. Mansour**, “A public –key encryption method implementation for wireless sensor networks (WSN)” Master Thesis, Computer Science Department, Jordan University of Science and Technology, Jordan, July 2012.
6. **H. Tawalbeh**, “Hardware Performance Evaluation Of Sha-3 Candidate Algorithms”. Master Thesis, Computer Science Department, Jordan University of Science and Technology, Jordan, June 2012.
7. **A. Alkaff**,” Hardware Implementation for Elliptic Curve Crypto (ECC) computations”. Master Degree research project, Computer Science Department, Jordan University of Science and Technology, Jordan, 2011.
8. **W. M. Kanakri**, ” Elliptic Curve Crypto-processor Implementation Using Efficient Calculations of Modular Multiplicative Inverse”. Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, January 2010.
9. **Q. S.Abu Al-Haija'**, “Efficient Algorithms for Elliptic Curve Cryptography Using New Coordinates Systems. Computer Engineering Department, Jordan University of Science and Technology, Jordan, December 2009
10. **S. F. Swaidan**, “Modular Squaring Algorithms Suitable for Hardware Implementations in GF(p). Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, December 2007.
11. **Y. I. Jararwah**, A hardware architecture of an Efficient Modular Division Algorithm for Cryptographic Applications. Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, July 2007.
12. **A. A. Mohammad**, “An Architecture for Elliptic Curve Crypto-processor for Programmable Hardware”. Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, July 2007.

13. **S. Z. Sweedan**, " Hardware Design and Implementation of Elgamal Public-Key Cryptography Algorithm," Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, Feb. 2007
14. **M. I. Salameh**, " A New and Efficient Key Distribution Protocol", Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, Feb. 2007

PhD STUDENTS SUPERVISED:

- No PhD Program for Computer Engineering at JUST.
-

MEMBER OF MASTER STUDENTS EXAMINATION COMMITTEE:

1. Liana Qabajeh," Distributed Secure Routing Protocol for Mobile Ad-Hoc Networks". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, Aug. 2005.
2. DeefALLAH Mohammad Al-Shorman," Evaluation of Image Edge Detection Using Fuzzy Set Theory and Neural Network to Detect Brain Cancer". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, July 2006.
3. Ahmad Nawasrah, "Adaptive Forward Error Correction Based on Probability of Loss and Recovery Rates". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, October 2006.
4. Ramzy Saifan," A Novel Algorithm for Defending The Denial of Service Attacks in Sensor Networks". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, November 2006.
5. Mohammed Al-Hammouri."Recognition of Dynamic Gestures in Arabic Sign Language Using HMM". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, December 2006.
6. Ahmad Arafat."Network Intrusion Detection System Using Attack Behavior Classification". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, December 2006.
7. Omar Migdadi," Power Aware Aodv Routing Protocol for Bluetooth Scatternet". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, January 2007.
8. Musab Alawneh," Complexity Related Aspects of Face Recognition". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, January 2007.
9. Mufleh Shatnawi," Hardware Implementation of Digital Oscillators Using Advanced Digital Arithmetic Techniques". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, March 2008.
10. Abdulraheem Mustafa," Countering P2P-Based Denial of Service Attacks". Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, May 2008.

PROFESSIONAL ACTIVITES

Journal Reviewer:

1. IEEE Transactions on Computers.
2. IEEE Transactions on VLSI Systems.
3. IET Circuits, Devices and Systems.
4. IEEE Potentials Magazine
5. Journal of System Architecture.
6. Integration, the VLSI Journal.
7. Information Security Journal; A global perspective.
8. International Journal of Modeling and Simulation.

Conference Reviewer:

1. ARITH-16 (16th IEEE Symposium on Computer Arithmetic, Santiago de Compostela, SPAIN, 2003).
2. The First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2008)-UK.
3. The Second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009)-UK.
4. International Conference on Information and Communication Systems (ICICS 2009).
5. Regular reviewer with the workshop on Cryptographic Hardware and Embedded Systems (CHES).
6. The 1st International Congress on Pervasive Computing and Management (ICPCM 2008)-Delhi, India).
7. The 2nd International Congress on Pervasive Computing and Management (ICPCM 2009)- Sydney, Australia.

International Conferences Committee Member

1. International Program Committee Member in The First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2008)-UK (Technical co-sponsored by IEEE UK and RI Region).
2. Technical Program Committee Member in the International Nuclear and renewable Energy Conference, Amman, Jordan 2009 (IEEE co-sponsored)
3. International Program Committee Member in The Second International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009)-UK (Technical co-sponsored by IEEE UK and RI Region).
4. Program Committee Member in the International Conference on Information and Communication Systems (ICICS 2009), Amman, Jordan.
5. Program Committee Member, in The 2nd International Congress on Pervasive Computing and Management (ICPCM 2009)- Sydney, Australia.
6. Program Committee Member International Conference on Information and Communication Systems (ICICS 11), Amman, Jordan.
7. International Program Committee Member in the International Conference on 'Networked Digital Technologies (NDT 2009) (technically co-sponsored by IEEE Communications Society), Czech Republic.

SENIOR GRADUATION PROJECTS SUPERVISED:

1. Moa'menah Alqudah and Ansam Abu-Dalo." Sixth Sense: The Physical World is Always Connected to The Digital World." 2010.
2. Mubarak Al-Qahtani and Mohamad Masoud," Hyper Arabic Computer Interface (HACI)". 2008
3. Doaa N. Mhiedat and Haya T. Rababa'ah. " Improved IDEA Algorithm". 2007.
4. Hanan Ammari, "Blowfish Encryption Algorithm with a Randomly Generated S-boxes". 2007.
5. Areej Almajali and Farah As'ad," IDEAL " An Improved Symmetric Encryption Algorithm Based on the International Data Encryption Algorithm". 2007.
6. Ayat Khatatbeh and Tasneem Abu-Qtaish,"New efficient crypto Algorithm design and Implementation (ALT)". 2007.
7. Shadi Alzoubi, "Voice Over Internet Protocol (VOIP)". 2007.
8. Abdelrahman Abdullah Mohammad."CDMA 1x EV-DV Security Layer, Phase 1: Encryption Protocol". 2006.
9. Dana Shatnawi, Rasha Al-Balawneh and Reham salman."Hardware Design for Radix-16 Montgomery Multiplication". 2006.
10. Amani Matekri and Shatha Abu-Laban," CDMA 1x EV-DV Security Layer: Phase 2: Authentication Protocol". 2006.
11. Alaa Badarneh, Samiha Falahat and Isra Badarneh."Hardware Design And Implementation Of BlowFish Cryptographic Algorithm". 2006.
12. Fawaz Khasawneh and Nooh Milhim." RSA Crypto processor" 2006.
13. Samir Alhasan."Bluetooth Control System using The Mobile". 2006

COURSES TAUGHT/CURRENTLY TEACHING (2005-NOW):

I taught a total of 18 Graduate courses and 8 Undergraduate courses at 5 universities:

At: Jordan University of Science and Technology (JUST) (FULL TIME):

Graduate Courses:

1. CPE 776 Security and Cryptography (Fall '11, Fall '10, Fall '08, Summer '06, Summer '05)
2. CPE 746 Embedded Systems Design (Fall '07, Fall '06)
3. CPE 779 Advanced Computer Arithmetic (Fall '12, Spring '08, Spring '06, Fall '05)

Under-graduate Courses:

4. CPE 552 Computer Design (Summer '12, Spring '11, Spring '10, Spring '09, Spring '07)
5. CPE 542 Cryptography and Network Security (Summer '08, Fall '05, Summer '05)
6. CPE 350 Hardware Description Language Lab (Summer '08)
7. CPE 312 Numerical Analysis (Spring '11, Spring '10, Spring '09, Spring '08, Fall '06, Fall '05, Spring '05)
8. CPE 252 Computer Organization and Design (Fall '12, Summer '11, Fall '10, Fall '09, Summer '09, Fall '08, Fall '07, Spring '07, Fall '06, Spring '06, Spring '05)

At: Umm Al-Qura University- Saudi Arabia:

Graduate Courses:

9. Information Security
10. Computer Forensics

Undergraduate Courses:

11. Cloud Infrastructure and Services
12. Numerical Engineering analysis
13. Computer Systems Security

At: New York Institute of Technology (NYIT) - Amman's Campus:

Graduate Courses:

14. INCS 745: Intrusion Detection and Hackers Exploits (Spring '11, Fall '08, Fall '07, Spring '07, Winter '07, Fall '06, Summer '06)
15. NCS 712: Computer Forensics (Summer '09, Summer '08, Spring '07, Fall '06, Spring '06)
16. NCS 741: Cryptography (Fall '11, Fall '07, Summer '07)
17. NCS 735: Secure Software Engineering (Summer '09)
18. EEN 755: Computer Networks (Summer '08)
19. CSCI 620: Operating System Security (Fall '09, Spring '09, Fall '08)
20. CSCI 860: Special Topics: Data Security & Cryptography (Spring '05)

At: Princes Sumaya University:

21. Cryptography
22. Network Security

At: Depaul University-Amman's Campus:

Graduate Courses:

23. TDC 512: Cellular and Wireless Communications. (Spring '07)
24. TDC 565: Voice and Data Integration. (Summer '07)
25. TDC 532: Wireless Systems Engineering and Deployment. (Winter '08)
26. TDC 577: Network Security. (Fall '08)

Community services

1. Organize and participate in the National gathering about Population and Mothers health: The road to achieve the Millennium development goals” Organized by AMAN-Jordanian association for family and society protection- Member at International Union for family management and protection. Feb 2010.
2. Organize and attend a regional workshop on “Applying best practices in family management techniques”, 2009.
3. Organize the first gathering about protecting youth form DRUGS and AIDS at Jordan University of Science and Technology for 5 days (I gave speeches on this subject to the University students). “Youth Protectors”, May 2007.
4. Organize a workshop “ The Role of Universities in protecting students from AIDS and DRUGS” at Jordan University of Science and Technology. May 2008.

DEPARTMENT AND COLLEGE COMMITTEE PARTICIPATION

1. Higher education and scientific research department committee (2009, 2010, 2011)
2. Students affairs department committee -2008
3. Engineering training department committee - 2010
4. Curriculum and courses equivalency department committee -2006, 2007
5. Master degree comprehensive exam department committee (to write the exam in three graduate courses: Network Security, Embedded Systems, Advanced Digital Arithmetic) (2007-2011)
6. Scholarships department committee-2006
7. Social activities department committee 2009
8. A committee to embed the Computer Aided Design tools in the curriculum-2010
9. Improvement of evaluation process COLLEGE committee-2007
10. Representative of computer engineering department at the COLLEGE council- 2007
11. Conferences and Scientific workshop COLLEGE committee-2008

LANGUAGES

Arabic: Native, **English:** Fluent

REFERENCE (Work Supervisors)

1. Dr. Fahd AlDosari:
Dean of College of Computer & Information Systems
Umm Al-Qura University
P.O. Box: 715
Makkah 21955, Saudi Arabia
Email: fmdosari@uqu.edu.sa

Mobile number: +966-505-528-288

2. Prof. Omar AL-Jarrah

Professor of Computer Engineering

2013-present: President – Open Arab University, Amman, Jordan.

Before 2013: Vice president: Jordan University of Science and Technology

PO. Box: 3030, Irbid 22110, Jordan

Phone: +(962) 795-692-223

Fax : +(962) (2) 7095046

email: aljarrah@just.edu.jo

3. Prof. Jalal Atoum.

From 2000-2010: Coordinator of the of Engineering and Information Technology program

Graduate Program in Information, Computer and Network Security

NewYork Institute of Technology-Jordan's Campus.

Amman, Jordan.

USA Phone: **+1-817-8914967**

Jordan Phone: +(962) 775-741-114

Email: atoum@psut.edu.jo,

4. Prof. Walid Salameh.

Professor of computer science (computer and network security), and Vide president.

Dean of Graduate Studies and Scientific Research at Princess Sumaya University for Technology,

Khalil Saket street, P O Box 1438,

Al-Jubaiha 11941, Amman, Jordan.

Mobile Number: +962-777-485-777.

Office number : +96 2 65356574 **Extension: 290**

Email: walid@psut.edu.jo

REFERENCE (International)

1. Prof. Cetin K. Koc, Full professor of Computer Engineering

University Of California-Santa Barbara, USA.

The director of the Information Security Lab at Oregon State University, USA –till 2008.

Email: koc@cryptocode.net, Email: koc@cs.ucsb.edu,

Cell: +1 805 403 4191.

<http://www.cs.ucsb.edu/~koc/>

2. Prof. Alexandre Tenca

Senior Engineer at Synopsys, USA.

Assistant professor in the Electrical and Computer Engineering Dept. at Oregon State University (OSU), USA till 2004.

Email: tenca@synopsys.com

3. Prof. Adnan Gutub.

Associate Professor in Computer Engineering, Umm Al Qura University, KSA.

Director of the *Center of Research Excellence in Hajj and Omrah*,
Email: aagutub@uqu.edu.sa