COMPUTER ENGINEERING DEPARTMENT
COLLEGE OF COMPUTER AND INFORMATION TECHNOLOGY
JORDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. BOX 22110
IRBID, JORDAN

DR.LO'AI A. TAWALBEH

DIRECTOR OF THE CRYPTOGRAPHIC HARDWARE AND INFORMATION SECURITY LAB (CHIS)

PHONE	+962-78-573-0072
	+962-77-641-4183
FAX	+962-2-709 5046
E-MAIL	tawalbeh@just.edu.jo
WEBSITE	www.just.edu.jo/~tawalbeh

PERSSONAL INFORMAITON:

- **Date of Birth:** May, 1977
- **Citizenship:** Jordanian
- **Marital status:** married with one kid

EDUCATIONAL QUALIFICATIONS:

October 2004

- **PhD.** in Electrical and Computer Engineering from Oregon State University (OSU), Corvallis, Oregon, USA. **GPA= 4.00/4.00.**

- 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

- **Masters** of Science in Electrical and Computer Engineering. Oregon State University, Corvallis, Oregon, USA. **GPA= 4.00/4.00**.

- Thesis Title: "Radix-4 ASIC Design of a Scalable Montgomery Modular Multiplier Using Encoding Techniques". October 24, 2002.

June 2000

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

Key Words: ***Cryptography, Information Security, Efficient Cryptographic Algorithms Design and Implementation in Hardware, Modular Arithmetic Algorithms, Elliptic Curve Cryptography, FPGA.***

RESEARCH INTERESTS:

- Cryptographic co-processor design using scalable modules
- Efficient cryptographic algorithms design and implementation
- FPGA design
- Arithmetic algorithms for cryptography
- Elliptic-curve cryptography design and implementations.
- Information, network and computer security
- Computer forensics tools and methodologies and Intrusion detection

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. Research Member at the Information Security Lab at Oregon State University, USA.
3. Research Member at the Machine Intelligence Research Lab, USA (started Jan. 2011).
4. Since I believe that the academia must NOT be separated from the Industry, I cooperated with some of my colleagues and established 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.

AWARDS AND GRANTS

- Research Grant: "Efficient Cryptographic Processor for Internet and Wireless Security Based on Elliptic Curve Cryptography"- 80,000$. July 2009-December 2010. Ministry of High Education-Jordan.
- Designing a co-processor for public-key and symmetric cryptographic applications using VHDL in ASIC and FPGA. Research supported by the National Science Foundation (NSF), USA CAREER grant CCR-0093434- "Computer Arithmetic Algorithms and Scalable Hardware Designs for Cryptographic Applications", USA, 2001.
- 9/2001 – 10/2004 National Scholarship to get master, doctoral degrees at Oregon State University, Corvallis, Oregon, USA.

MEMBERSHIP OF SCIENTIFIC AND PROFESSIONAL SOCIETIES

1. IEEE, and IEEE Society Member 2001-2005.
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.

SCHOLARSCHIPS

- National Scholarship from Jordan University of Science and Technology to get master degree at Oregon State University, Oregon, USA, October 2001.
- National Scholarship from Jordan University of Science and Technology to get Doctoral degree at Oregon State University, Oregon, USA, October 2002.
- Research Assistant Scholarship from Oregon State University, USA, 2002-204.

SELECTED PUBLICATIONS:

Journal Papers:

1. **L. A. Tawalbeh. "**Arithmetic Algorithms and Hardware designs for cryptography", Submitted to *The IEEE Transactions on Parallel and Distributed Systems*. 2011.

2. **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". Submitted to the *Information Sciences Journal*. Elsevier, Jan. 2011.

3. **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*, Dynamic Publishers, Inc., USA. Accepted January 2011.

4. Q. A. Al-Haija and **L. A. Tawalbeh**. "Efficient Algorithms & 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, 2011.

5. **L. A. Tawalbeh** and Sae'deh 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.

6. **L. A. Tawalbeh**, Abidalrahman Mohammad and Adnan A. Gutub. "Efficient FPGA Implementation of a Programmable Architecture for GF(p) Elliptic Curve Crypto Computations". *Journal of Signal Processing Systems*, Vol (59) Number (3), pages 233-244. Springer, June 2010.

7. **L. A. Tawalbeh**, Yaser Jararweh and Abidalrahman Moh'md. "An Integrated Radix-4 Modular Divider/Multiplier Hardware Architecture for Cryptographic Applications". *The International Arab Journal of Information Technology*, Accepted June 2010.

8. F. Bin Muhaya, Q. Abu 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.

9. **L. A. Tawalbeh**, Saed Swedan, Adnan 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.

10. 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, number 5 pages 630-636, May 2006.

11. **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.

12. A. Tenca and **L. A. Tawalbeh** "An Algorithm for Unified Modular Division in GF(p) and GF(2^n) Suitable for Cryptographic Hardware". *IEE Electronics Letters*, 40(5),304-306, March 2004.

Book Chapter:

13. **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.

Conference Papers:

14. Abidalrahman 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.
15. **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.
16. **L. A. Tawalbeh**, Mohamd Alrousan, and Doa Alansari, "Survey of efficient public-key management schemes for wireless sensor networks" ICPCM 2009, Sydney- Australia. Dec. 12-14, 2009.
17. Abidalrahman 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.
18. A. A. Mohammad and **L. A. Tawalbeh**."A Modified Version of the Advanced Encryption Standard Algorithm with Extra Key Size and Block Size". In the 1st International Conference on Digital Communications & Computer Applications. JUST, Jordan, March, 19-22 2007.
19. Mohamamd Alrousan, **L. A. Tawalbeh** and Khaled Al-Saleh,"Voice-Driven Smart Wheel Chair. In The Third AUS-International Symposium on Mechatronics. Sharjah, UAE, April 18-20, 2006.
20. **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, August 2-4, 2005.
21. Abdoul 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.
22. **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.
23. **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.
24. 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.

CITATIONS

The above papers have been cited more than **27** times (exclude self citations) in journal and conference publications, as well as in patents, technical reports and dissertations. Some of these citations can be found bellow:

US Patent:

1. ***Reference [4] in:*** United States Patent, Son. "Montgomery Modular Multiplier". US. Patent no. 7,805,478. Sept. 28, 2010. http://www.patentgenius.com/patent/7805478.html

Journals:

2. ***References [24, 25] in:*** Bajard, J.-C.; Negre, C.; Plantard, T.; , "Subquadratic Space Complexity Binary Field Multiplier Using Double Polynomial Representation," *IEEE Transactions on Computers*, vol.59, no.12, pp.1585-1597, Dec. 2010. doi: 10.1109/TC.2010.141. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5487504&isnumber=5611468
3. ***Reference [16] in*** : A. Ibrahim and et al.," Processor Array Architectures for Scalable Radix 4 Montgomery Modular Multiplication Algorithm," *IEEE Transactions on Parallel and Distributed Systems*, 08 Nov. 2010. IEEE computer Society Digital Library. IEEE Computer Society. http://www.computer.org/portal/web/csdl/doi/10.1109/TPDS.2010.196
4. ***Reference [23] in:*** Chia-Long Wu,"Fast exponentiation based on common-multiplicand-multiplication and minimal-signed-digit techniques", International Journal of Computer Mathematics, pp.1405-1415, vol. 84 Issue 10, October 2007, Taylor & Francis, Inc., USA. http://portal.acm.org/citation.cfm?id=1393360.1393362
5. ***Reference [32] in:*** C. McIvor, M. McLoone, and J. McCanny, "Hardware Elliptic Curve Cryptographic Processor Over GF(p)". IEEE Transactions on Circuits and Systems I: Regular Papers, pp. 1946 - 1957, Volume: 53 Issue: 9, Sept. 2006**..** http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1703780
6. ***Reference [34] in:*** D. M. Schinianakis and et al., "An RNS implementation of an Fp elliptic curve point multiplier". IEEE Transactions on Circuits and Systems Part I-Regular Papers. Volume 56 Issue 6, June 2009**..** Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4663678
7. ***Reference [52] in:*** E. Savas and C. Koc. "Finite field arithmetic for cryptography", IEEE Circuits and Systems Magazine, vol. (10) Issue (2), pp.40-56, 2010**..** http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5470228
8. ***Reference [19] in:*** A. Ibrahim, F. Gebali, H. El-Simary and A. Nassar, "High-performance, low-power architecture for scalable radix 2 Montgomery modular multiplication algorithm," *Canadian Journal of Electrical and Computer Engineering*, vol.34, no.4, pp.152-157, Fall 2009. URL: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5599422
9. ***Reference [8] in:*** D. Sangwan and M. Yadav. "Design and Implementation of Adder/Subtractor and Multiplication Units for Floating-Point Arithmetic", International Journal of Electronics Engineering, 2(1), 2010, pp. 197-203. http://www.csjournals.com/IJEE/PDF%202-1/40.pdf
10. ***References [30, 31] in:*** A Gutub. "Preference of Efficient Architectures for GF (p) Elliptic Curve Crypto Operations using Multiple Parallel Multipliers". International Journal of Security, CSC Journals, vol. 4 Issue 4, 2010..
URl:http://www.cscjournals.org/csc/manuscript/Journals/IJS/volume4/Issue4/IJS-52.pdf

Conferences:

11. ***Reference [8] in:*** D. Harris and et al., "An Improved Unified Scalable Radix-2 Montgomery Multiplier," arith, pp.172-178, 17th IEEE Symposium on Computer Arithmetic (ARITH'05), 2005. Available at: http://www.computer.org/portal/web/csdl/doi/10.1109/ARITH.2005.9

12. ***Reference [15] in:*** A. Wang, Y. Jin and S. Li, "Dual residue Montgomery Multiplication", Proceedings of the 2007 IFIP international conference on Network and parallel computing (NPC'07), LNCS 4672, pp. 267-276, Springer-Verlag, Berlin, 2007. http://www.springerlink.com/content/m13rj23j23531837/

13. ***Reference [14] in:*** K. Kelley and D. Harris. "Parallelized Very High Radix Scalable Montgomery Multipliers. In the Proc. of thirty-ninth Asilomar Conference on Signals, Systems, and Computers, pp.1196-1200, IEEE Press, California, Pacific Grove, USA, October 30-November 2, 2005. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.67.9768

14. ***Reference [20] in:*** Chia-Long Wu," Fast Parallel Montgomery Binary Exponentiation Algorithm Using Canonical- Signed-Digit Recoding Technique" Proceedings of the 9th International Conference on Algorithms and Architectures for parallel Processing (ICA3PP'09), Taiwan, June 2009. LNCS 5574, pp428-438, Springer-Verlag, Berlin, 2009. http://portal.acm.org/citation.cfm?id=1615051

15. ***Reference [4] in:*** N. Pinckney and D. Harris. "Parallelized Radix-4 Scalable Montgomery Multipliers". Proceedings of the 20th annual conference on Integrated circuits and systems design, Rio de Janeiro, Brazil, Sept. 3-6, 2007. Available at: http://portal.acm.org/citation.cfm?id=1284480.1284562

16. ***Reference [1] in:*** F. Fiaz and S. Masud, "Design and Implementation of a Hardware Divider in Finite Field", In the IEEE/ACM National Conference on Emerging Technologies, Pakistan, Dec. 18th, 2004 **.** Available at: http://www.szabist.edu.pk/ncet2004/

17. ***Reference [19] in:*** A. Ibrahim and et al.," New processor array architecture for scalable radix 2 Montgomery modular multiplication algorithm," *Communications, Computers and Signal Processing, 2009. PacRim 2009. IEEE Pacific Rim Conference on* , vol., no., pp.365-370, 23-26 Aug. 2009. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5291345&abstractAccess=no&userType=inst

18. ***Reference [4] in:*** P. Amberg, and et al.," Parallel High Radix Montgomery Multipliers". In the Proc. of 42nd Asilomar Conference on Signals, Systems, and Computers, pp.772-776, IEEE Press, California, USA, October 26-29, 2008. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5074513&abstractAccess=no&userType=inst

19. ***Reference [19] in:*** Johann Großschädl, Erkay Savas, Kazim Yumbul, "Realizing Arbitrary-Precision Modular Multiplication with a Fixed-Precision Multiplier Datapath," reconfig, pp.261-266, 2009 International Conference on Reconfigurable Computing and FPGAs, Mexico, Dec 9-11, 2009. Available at: http://www.computer.org/portal/web/csdl/doi/10.1109/ReConFig.2009.83

20. ***Reference [16] in***: S. Bartolini, G. Castagnini, and E. Martinelli. "Inclusion of a Montgomery Multiplier Unit into an Embedded Processor's Datapath to Speed-up Elliptic Curve Cryptography," Third International Symposium on Information Assurance and Security (IAS 2007), pp.95-100. UK, 29-31 Aug. 2007. http://www.computer.org/portal/web/csdl/doi/10.1109/IAS.2007.81

21. ***Reference [4] in:*** N. Pinckney and et al., "Parallelized Booth-EncodedRadix-4 Montgomery Multipliers," IFIP/IEEE VLSI SOC 2008, Rhodes Island, Greece, October 13-15, 2008**.** Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.158.5555

22. ***Reference [10] in*****:** K Kelley and D Harris."Very high radix scalable Montgomery multipliers", In the proceedings of the Fifth IEEE International Workshop on System-on-Chip for Real-Time Applications, DOI: 10.1109/IWSOC.2005.111, pp.400-404. Canada, July, 20-24, 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1530980&abstractAccess=no&userType=inst

23. T. Adiono and et al., "64-point fast efficient FFT architecture using Radix-23 single path delay feedback", Electrical Engineering and Informatics, 2009. ICEEI '09. International Conference, vol. 2, pp. 654 – 658, Selangor , Malaysia, Aug. 5-7, 2009. (I wasn't able to access this paper to know the reference number). http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5254734&abstractAccess=no&userType=

24. Yehua Gu; Xiaoyang Zeng; Jun Han; Yongxin Ma; Jia Zhao; , "A Scalable Design of RSA Crypto-coprocessor," *8th International Conference on Solid-State and Integrated Circuit Technology, 2006. ICSICT '06*, pp.1889-1892, 23-26 Oct. 2006. (I wasn't able to access this paper to know the reference number). http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4098572&abstractAccess=no&userType=inst

Master Theses:

25. ***References [7, 8, 14] in:*** S. Park. "Hardware design of scalable and unified modular division and Montgomery multiplication". Master thesis, Department of electrical and computer engineering, Oregon State University, June, 6th, 2005. Available at: http://scholarsarchive.library.oregonstate.edu/xmlui/handle/1957/10220
26. ***References [9] in:*** E. Kair."The design of a test environment and its use in verification of a scalable modular multiplication and exponentiation". Master thesis, Department of electrical and computer engineering, Oregon State University, March 2004. http://ir.library.oregonstate.edu/xmlui/handle/1957/10213

Technical Reports:

27. ***References [37] in:*** A. Gutub and T. Kalganova. "Speeding up a scalable modular inversion hardware architecture". Research Final report-British Council Research Program, 2005. http://uqu.edu.sa/files2/tiny_mce/plugins/filemanager/files/4310001/reports/BC_Report_2005.pdf

TRAINING AND CERTIFICATES

1. Certified Ethical Hacking Training workshop (CEH)- April 2009.
2. Specialized workshop on "Creativity and Innovation". June 2006.
3. Training workshop on "Preparation the Leaders of Information Technology", Feb. 2006.
4. Training workshop on "Testing and Evaluation (University Examination Methodologies)".,July, 2005.
5. Java Certified Programmer, 2001

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.
9. Kuwait Journal of Science and Engineering.

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.

MASTER STUDENTS SUPERVISED (MAIN ADVISOR):

1. **M. I. Salameh**, " A New and Efficient Key Distribution Protocol", Master Thesis, Computer Engineering Department, Jordan University of Science and Technology, Jordan, Feb. 2007.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.

MEMBER OF MASTER STUNDENTS EXAMINATION COMMITTEE:

1. Liana Qabajeh," Distributed Secure Routing Protocol for Mobile Ad-Hoc Netwroks". 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 Netwroks". 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.

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 Mohamamd 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 Khasawenah and Nooh Milhim." RSA Crypto processor" 2006.
13. Samir Alhasan."Bluetooth Control System using The Mobile". 2006

PhD STUDENTS SUPERVISED:

- No PhD Program offered in Computer Engineering major at JUST.

COURSES TAUGHT/CURRENTLY TEACHING (2005-NOW):

I taught a total of 18 Graduate courses and 6 Undergraduate courses at 4 different universities:

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

Graduate Courses:

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

Under-graduate Courses:

4. CPE 552 Computer Design (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 '10, Fall '09, Summer '09, Fall '08, Fall '07, Spring '07, Fall '06, Spring '06, Spring '05)

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

Graduate Courses:

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

Under-Graduate Courses:

16. EENG 401: Communication Theory (Winter '07, Winter '06)

At: Depaul University-Amman's Campus:

Graduate Courses:

17. TDC 512: Cellular and Wireless Communications. (Spring '07)
18. TDC 565: Voice and Data Integration. (Summer '07)
19. TDC 532: Wireless Systems Engineering and Deployment. (Winter '08)
20. TDC 577: Network Security. (Fall '08)

At: The Arab Academy for Banking and Financial Sciences-Amman's Campus (Graduate):

21. ISS 6809: Information System Security (Summer '06) for PhD Students.
22. ISS 6750: Intrusion Detection (Spring '07) for Master students
23. ISS 6753: Security Risk Analysis (Spring '07) for Master students
24. ISS 6751: Policy Analysis and Program Evaluation (Summer '07, Fall '07) for Master students.

VISITING PROFESSOR

1. **2005-2010:** Part time professor at New York Institute of Technology (NYIT) - Amman's Campus, Jordan.
2. **2007-2009:** Part time professor at Depaul University - Amman's Campus, Jordan.
3. **2006-2007:** Part time professor at The Arab Academy for Banking and Financial Sciences- Amman's Campus, Jordan.

COORDINATIONS:

1. Coordinate a professional visit: professor Cetin K. Koc from University of California at Santa Barbara to Jordan University of Science and Technology, December 2009.
2. Coordinate a Professional visit: Mentor Graphics director of the Higher Education Program to Jordan University of Science and Technology, 2007.

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 " 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 (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. Milos Ercegovac, Full professor of Computer Science.**
   Chair of Computer Science department at University of California; Los Anglos, USA.
   Email: milos@cs.ucla.edu
   Phone: +1 310-825-5414
   http://www.cs.ucla.edu/~milos/

3. **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

4. **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

REFERENCE (Local)

5. **Prof. Omar AL-Jarrah**
   Vice president - a professor of Computer Engineering,
   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

6. **Prof. Mohamamd Al-rousan**
   Dean of the College of Computer and Information Technology, Professor of Computer Engineering,
   Jordan University of Science and Technology
   PO. Box: 3030, Irbid 22110, Jordan,
   Phone: +(962) 799-096-034
   Email: alrousan@just.edu.jo

7. **Prof. Jalal Atoum.**
   Dean of the Computer Science and Engineering Faculty at NYIT-Amman-till 2010.
   Princes Sumaya University for Technology, Amman, Jordan.
   Phone: +(962) 777-485-656
   Email: atoum@psut.edu.jo, Email: jatoum@nyit.edu.jo

8. **Prof. Walid Salameh.**
   Professor of computer science (computer and network security),
   Dean of Graduate Studies and Scientific Research Deanship at Princess Sumaya University for Technology**,** Amman, Jordan.
   Email:walid@psut.edu.jo