

## Dr. Reza Ebrahimi Atani

---

Computer Engineering Department  
University of Guilan  
Postal Code: 41996-13769  
P.O.Box: 41635-3756

Phone: +98-131-6690270 (3017)  
Mobile: +98 911-1485220  
Fax: +98-131-6690271  
rebrahimi@guilan.ac.ir,  
rebrahimi@ieee.org

Rasht, Iran

Webpage: <http://staff.guilan.ac.ir/rebrahimi/index.php?a=0&lg=1>

### Biographical Data

Birth date: 4th Sep. 1980

Place of Birth: Arak, Iran

Citizenship: Iranian

Marital Status: Married

### Education

PhD, May 2010

**Iran University of science and Technology,**

Electrical Engineering Department

Major: Deasign and Implementation of a Stream Cipher Design for Mobile communication

Supervisor: Prof. S. Mirzakuchaki

Advisor: Prof. S. Ebrahimi Atani (University of Guilan)

Thesis evaluation: 19.8 on 20 Scale.

Master of Science, Nov. 2004

**Iran University of Science and Technology**

Electrical Engineering Department

Major: VLSI design (Design and Implementation Of a General Purpose DSP Core)

Advisor: Dr S. Mirzakuchaki

Total GPA: 17.44 on 20 Scales

Bachelor of Science, Sep. 2002

**The University of Guilan**

Electrical Engineering Department

Major: Sigma Delta A/D converters.

Total GPA: 15.92 on 20 Scale

### Research and work Experience

**Assistant Professor**

Computer Engineering Department

from May. 2010

University of Guilan, Rasht, Iran

## **Dr. Reza Ebrahimi Atani**

---

**Director of Electronic Learning Office**  
University of Guilan

from July. 2011  
University of Guilan, Rasht, Iran

**Head of The Computer Engineering Group**  
Guilan Science and research Branch, Islamic  
Azad University

from November 2012  
Islamic Azad University, Rasht, Iran

**Head of The Information Technology  
Group**  
University of Guilan Pardis International Branch

from October. 2012  
University of Guilan, Rasht, Iran

**Lecturer**  
Electrical Engineering Department  
Teaching: Micro-Electronic Circuits, Electronic II Labrotary.

from Feb. 2010 to May 2010  
University of Guilan, Rasht, Iran

**Project Manager**  
IDRO & ERC-IUST

June 2009 – Dec. 2009  
VLSI Design Lab., Microelectronic Research and  
Development Center of Iran (MERDCI),  
Amirabad - Tehran, Iran

Design and Implementation of National FPGA

**Research Assistant**  
Prof. Sattar Mirzakuchaki

Dec. 2008 – Aug. 2010  
Circuit Design Lab., Electronic Research Center,  
Iran University of Science and Technology,  
Narmak - 16846, Tehran, Iran

Cryptographic Hardware and Embedded Systems - CHES.

**International Scholar**  
Prof. Ingrid Verbauwhede and Prof. Bart Preneel

Jun. 2008 – Dec. 2008  
Katholieke Universiteit Leuven, ESAT  
SCD/COSIC, Heverlee, Belgium

Cryptographic Hardware and Embedded Systems - CHES.

**Visiting Scholar**  
Willi Meier

Nov. 2007 – Jun. 2008  
FHNW, Windisch, Switzerland

Design and cryptanalysis of stream ciphers.

**Lecturer**  
Electrical Engineering Department  
Teaching: VLSI Design(Graduate), Electrnic 1, Electronic 1,3 Labrotaries.

2006–2007  
University of Guilan, Rasht, Iran

**Lecturer**  
Electrical Engineering Department  
Teaching: Electrnic 1, Electronic 2, Signals & Systems.

2006–2007  
Azad University of Boushehr, Boushehr, Iran

**Part Time Lecturer**  
Electrical & Computer Engineering Department

2004–2007  
Iran University of Science and Technology,  
Tehran, Iran

Teaching: VLSI Design, Electronic Lab1, Microprocessor Lab.

**Part Time Engineer**

SA Iran  
R&D.

2005–2006

Iran Communication Industries, Tehran, Iran

**Research Assistant**

Prof. Sattar Mirzakuchaki

Sep. 2002 – Nov. 2007

Circuit Design Lab., Electronic Research Center,  
Iran University of Science and Technology,  
Narmak - 16846, Tehran, Iran

VLSI Design.

**Part Time Researcher**

ICII R&D Department

April 2003–Nov 2004

Iranian Telecommunication Research Center,  
Tehran, Iran

Design and Implementation of a DSP Processor on FPGA.

**Summer Internship**

Guilan Tele-Communication Center

Summer 2001

Rasht, Iran

Working as a technician (ASR and KIATEL communication Switches)

## Teaching Experience

### Graduate Courses

**Advance Computer Networks** in the **University of Guilan**, 5 Semesters.

**Network Security** in the **University of Guilan**, 2 Semester.

**Security Issues in Electronic Commerce** in the **University of Guilan**, 5 Semesters.

**Software Fault Tolerance Design** in the **University of Guilan**, 2 Semester.

**Electronic Payment Systems** in the **University of Guilan**, 1 Semesters.

**Electronic Banking** in the **University of Guilan**, 5 Semesters.

**VLSI Design** in the **University of Guilan**, 1 Semester.

### Bachelor Courses

**Discrete Mathematics** in the **University of Guilan**, 1 Semesters.

**Computer Networks** in the **University of Guilan**, 4 Semesters.

**Digital Electronics** in the **University of Guilan**, 2 Semesters.

**Digital Design** in the **University of Guilan**, 2 Semesters.

**Electronics I** in the **University of Guilan**, 7 Semesters.

**Microelectronic Circuits** in the **University of Guilan**, 3 Semesters.

**Electronic II Lab** in the **University of Guilan**, 2 Semesters.

**Electronic II** in **Azad University of Boushehr**, 2 Semesters.

**Signals And Systems** in **Azad University of Boushehr**, 1 Semesters.

**VLSI Design** in **Iran University of Science and Technology and University of Guilan**, 6 Semesters.

**Electronic III Lab** in the **University of Guilan**, 1 Semesters.

**Microprocessor Lab** in **Iran University of Science and Technology**, 2 Semesters.

**Electrical Circuits I** in **Shahid Rajai University**, 2 Semesters.

### **Research Interests**

1. Design and Analysis of Cryptographic primitives (Stream Ciphers, Block Ciphers, Hash Functions)
2. Computer Security
3. Cryptographic Hardware and Embedded System (CHES)
4. Semi-Rings, Semi-Modules, Ideal Theory
5. Public Key Cryptography
6. Steganography
7. Information Hiding
8. Network Security

### **Membership**

IACR : International Association for Cryptologic Research (Member No. 20070771) 2008 - 2013.

IEEE : Institute of Electrical and Electronics Engineers, Inc. (Member No. 90376818) 2008 - 2013.

IEEE : Communications Society (Member) 2008 - 2010.

ISC : Iranian Society of Cryptology (Member No. 660) 2007 - 2013.

IACSIT : International Association of Computer Science and Information Technology (Senior Member No. 80340217) Since 2010.

AIRCC : Academy & Industry Research Collaboration Center (Member No. 128512) Since 2010.

SDIWC : The Society of Digital Information and Wireless Communications Since 2010.

### **Relevant Computer Experience**

#### **Packages or CAD tools:**

MATLAB (Simu-Link), Cadence, HSPICE, PSPICE, PROTEL, ORCAD.

#### **VHDL, Verilog and related software:**

MODELSIM, MAXPLUS II, Design Vision, Leonardo Spectrum, Quartus, ISE, Active HDL, Simplorer, Synplify.

#### **Programming languages:**

80X86 ASSEMBLY, C/C++, Visual Basic, Web Developing Tools.

#### **Microprocessors and Micro-controllers:**

Z80, 80x86 microprocessors and the 8051 micro-controller, AVR, FPGA

### **Presented Workshops**

1. **“Modern Banking and the Security of new Electronic Banking Services,”** National Conference On information And Communication Security, Ahwaz, Iran, December 2010. (4h Talk)
2. **“Physical Attacks on Cryptographic Hardware and their Countermeasures,”** National Conference On information And Communication Security, Ahwaz, Iran, December 2010. (4h Talk)
3. **“Secure Hardware design: Attacks on Cryptographic Hardware and their Countermeasures,”** ISCISC 2010 conference, Tehran, Iran, September 2010. (4h Talk)

## Presentations

1. **“Low Cost Implementation of Pomaranch S-Boxes,”** WirelessVITAE’09, May 17-20, 2009, Aalborg, Denmark.
2. **“Alamout: A new Synchronous stream cipher with Authentication,”** WirelessVITAE’09, May 17-20, 2009, Aalborg, Denmark.
3. **“Design and Simulation of a DPA Resistive Circuit for Trivium Stream Cipher Based on SABL Logic Styles,”** MIXDES’08, Poznan, 19-21 June 2008, Poland.
4. **“Design and Implementation of DPA Resistive Grain-128 Stream Cipher Based on SABL Logic,”** ICCCC’08, 15-17 May, 2008, Flix Spa, Romania.
5. **“Countermeasures Against DPA Attack for Two eSTREAM Candidates on Cell Level,”** FHNW (Switzerland), 8th Feb. 2008.
6. **“Vision Chips,”** Iran University of Science and Technology, June 2005.
7. **“Design and Simulation of a 10 MHZ DSP Processor and Implementing it on ACTEL FPGA”**, Iran University of Science and Technology, Nov. 2004.
8. **“Substrate Cross Talk Effect in Mixed Signal Design,”** Iran University of Science and Technology, Fall 2003
9. **“Digital Signal Processing using FPGA”**, Iran University of Science and Technology, Summer 2003.

## Honors and Awards

Best Researcher Award (September 2012) University of Guilan, Rasht, Iran.

Best reviewer Award (September 2010) ISCISC 2010, Tehran, Iran.

Awarded Scholarship for 6 month (Jun. 2008- Dec. 2008) from Katholieke Universiteit Leuven, ESAT SCD/COSIC, Belgium for International Scholar position.

Awarded Sabbatical Scholarship for 9 Month (Nov. 2007- August 2008) from the Iranian Ministry of Science, Research and Technology for Visiting FHNW - Switzerland.

Awarded Doctoral Scholarship for 3.5 year (Sep. 2005- March 2009) from the Iranian Ministry of Science, Research and Technology (Grant No. 42.4.15146).

Awarded scholarship for PhD project through Iran Tele-communication Research Center (ITRC) 2007.

Awarded scholarship for Msc project through Iran Tele-communication Research Center (ITRC) 2004.

Ranked 220th among 17,000 other participants in electronics in national postgraduate studies entrance exam, held by the ministry of education.

Ranked 151th among 400,000 other participants in Math and Physics in national university entrance exam (concourse) held by the ministry of education.

## Language Skills

Farsi: Mother tongue

English: Advanced

## Publication

### Journal papers

1. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "On semiprime multiplication modules over pullback rings", *Communications in Algebra*, Vol.41, Issue 2,(2013), Pages: 776-791.
2. Abdolrahman Attar, Reza Moradirad, Reza Ebrahimi Atani, A survey of Image spamming and filtering techniques, *Artificial Intelligence Review*, Volume 40, Issue 1, (2013), Pages: 71-105.
3. Reza Ebrahimi Atani, "Generalizations of Prime Ideals of Semirings", *Azerbaijan Journal of Mathematics*, Vol. 3, No. 1, (2013), Pages: 76-83.
4. Reza Moradi Rad, Abdolrahman Attar, Reza Ebrahimi Atani, "A Comprehensive Layer Based Encryption Method for Visual Data", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 6, No. 1, (2013), Pages: 37-48.
5. Mohammad Sabzinejad Farash, Mahmoud Ahmadian Attari, Reza Ebrahimi Atani, Mohamadreza Jami, "A new efficient authenticated multiple-key exchange protocol from bilinear pairings", *Computers and Electrical Engineering*, Vol. 39, Issue 2, February 2013, Pages: 530541.
6. Amir Hassani Karbasi, Reza Ebrahimi Atani, "APPLICATION OF DOMINATING SETS IN WIRELESS SENSOR NETWORKS", To Appear in the *International Journal of Security and Its Applications*.
7. Seyed Mehrzad Almasi Mousavi, Hamid Reza Naji, Reza Ebrahimi Atani, "Optimization of majority protocol for controlling transactions concurrency in distributed databases by multi-agent systems", *International Journal of Applied Operational Research*, Vol. 2, No. 4 (2013), pp. 95-109.
8. Ramin Bahrapour, Reza Ebrahimi Atani, "A Novel Key Management Protocol for Wireless Sensor Networks Based on PUFs", *International Journal of Future Generation Communication and Networking*, Vol. 6, No. 2, April, 2013, Pages: 93-106.
9. Reza Ebrahimi Atani, "The L-total Graph of an L-module", *ISRN Discrete Mathematics*, Volume 2011 (2011), Pages: 1-10, doi:10.5402/2011/491936.
10. Ali Ahmadian Ramaki, Reza Ebrahimi Atani, "Language Based Security to Apply Computer Security", *International Journal on Cryptography and Information Security (IJCIS)*, Vol.2, No.3, September 2012, Pages: 37-47.
11. Ali Ahmadian Ramaki, Reza Asgari, Reza Ebrahimi Atani, "Credit Card Fraud Detection Based on Ontology Graph", *International Journal of Security, Privacy and Trust Management ( IJSPTM)*, Vol. 1, No 5, October 2012, Pages: 1-12.
12. Reza Asgari, Ali Ahmadian Ramaki, Reza Ebrahimi Atani and Asadollah Shahbahrami, "Multi Objective Design Space Exploration for Grid ALU Processor", *International Journal of Embedded Systems and Applications (IJESA)*, Vol.2, No.3, September 2012, Pages: 23-35.
13. Ali Ahmadian Ramaki, Reza Ebrahimi Atani, "Alert Correlation for Computer Network's Intrusion Detection in Distributed Environment", (under review).
14. Reza Asgari, Reza Ebrahimi Atani, "Anomaly Detection In Databases Based On Ontology Graph", *International Journal on Cybernetics & Informatics ( IJCI)*, Vol. 1(5), 2012, Pages: 1-10.
15. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani "Spectra of semimodules", To appear in the *Buletinul Academiei de tiine a Republicii Moldova, Matematica*, Vol. 67(3) (2011), Pages: 15-28.
16. Asghar Mokhtari, Mehregan Mahdavi, Reza Ebrahimi Atani, Mahrokh Maghsoudi, "Using Capture Effect in DFSA Anti-collision Protocol in RFID Systems According to ISO18000-6C Standard", *Majlesi Journal of Mechatronic Systems* Vol. 6, No. 2, June 2012.

17. Zahra Ghane Fashtali, Mahrokh Maghsoudi, Reza Ebrahimi Atani, Mehregan Mahdavi, "0.5-7.5 GHz Low-Power, Inductorless Current Folded Mixer In 0.18- $\mu$ m CMOS For Broadband Applications", International Journal of Electrical and Electronics Engineering (IJEEE), Vol. 1, Iss-4, 2012, Pages: 108-112.
18. Somayeh Izadi, Saeed Zahedi, Reza Ebrahimi Atani, A novel Secure Protocol ,IES, For Mobile Voting, IOSR Journal of Engineering (IOSRJEN), Vol. 2(8), Pages: 6-11, August 2012.
19. Somayeh Izadi, Reza Ebrahimi Atani, Mobile Voting (Chance or Challenge), IOSR Journal of Engineering (IOSRJEN), Vol. 2(8), Pages: 1-5, August 2012.
20. Somayeh Izadi, Saeed Zahedi, Kamran Morovati, Reza Ebrahimi Atani, Hadi Foroutan Jazi, Advanced in Mobile Voting, International Journal of Advanced Research in Computer Science (IJARCS), Vol. 3(5), Pages: 127 - 131 (2012).
21. Maryam pirouz, Mehregan Mahdavi, Reza Ebrahimi Atani and Maziar Salahi, Operational Risk Evaluating and Modeling for e-Banking, International Journal of Advanced Research in Computer Science (IJARCS), Vol. 3, No.3, Pages: 1-4, May 2012.
22. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani, "A Zariski topology for k-semirings, To appear in the Quasigroups and Related Systems, Vol. 20(1), (2012), Pages: 29-36.
23. Sara Salehi Mahboub, Seyed Mohammad Asadinejad, Reza Ebrahimi Atani, "A Novel Secure Smart Student Card Model Case Study: Guilan University", Journal of Computing, VOL. 3, ISSUE 12, Dec 2011, Pages: 108-112.
24. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "On primarily multiplication module over pullback ring", Algebra and Discrete Mathematics, Vol. 11 (2011) No.1.
25. Saeed Mehmandoust, Reza Ebrahimi Atani, "Application of PUF-enabled RFID Tags In Electronic Banking", to appear in the International Journal of Computer Science & Information Technology, Vol. 3. No. 2, (2011), Pages: 191-202.
26. Farzad Tavakkoli, Azam Andalib, Asadollah Shahbahrami, Reza Ebrahimi Atani, "A Comparison of Lightweight Databases in Mobile Systems", To appear in the Journal of Computing, Volume 3, Issue 7, July 2011, Pages: 147 -152.
27. Farzad Tavakkoli, Reza Ebrahimi Atani, Shahriar Mohammadi, "A Novel Model for Secure Mobile SMS Banking", International Journal of Information Assurance and Security, Vol. 6, Issue 4, (2011), Pages: 369-378.
28. Mehdi Ayat, Reza Ebrahimi Atani, Sattar Mirzakuchaki, "On Design of PUF-Based Random Number Generators", To appear in the International journal of Network Security & Its Applications (2011).
29. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani, Unsal Tekir, "A Zariski Topology for Semi-modules", European Journal of Pure and Applied Mathematics, Vol 4(3) (2011), Pages: 251-265.
30. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani, "On strong QR-ideals of commutative semirings", to appear in the Journal of Advanced Research in Pure Mathematics (JARPM) (2011).
31. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani " On DPA-Resistive Implementation of FSR-based Stream Ciphers using WDDL Logic Styles", International Journal on Communications Antenna and Propagation (IRECAP), Vol. 1, No. 1, (2011), Pages: 83-91.
32. Shahriar Mohammadi, Reza Ebrahimi Atani and Hossein Jadidoleslami, "A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security (JIS), Vol. 2, No. 2, (2011), Pages: 69-84.
33. Shahriar Mohammadi, Reza Ebrahimi Atani and Hossein Jadidoleslami, "A Comparison of Routing Attacks on Wireless Sensor Networks", International Journal of Information Assurance and Security, Vol. 6, Issue 3, (2011), Pages: 195-215.
34. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani "Graded multiplication modules and the ideal  $\theta_g(M)$ ", Turkish Journal of Mathematics, Vol. 35, Issue 1, 2011, Pages: 1-9.

35. Gholamreza Karimi, Reza Ebrahimi Atani, Abolfazl Taleb Bayghi "A Novel Design Technique to Speed-up the Charge Pump and improve the Stability of PLLs", *International Review on Computers and Software (IRECOS)*, Vol. 5(6), (2010), Pages: 671-679.
36. Reza Ebrahimi Atani, "Prime Subsemimodules of Semimodules", *International Journal of Algebra*, Vol. 4, 2010, no. 26, Pages: 1299 – 1306.
37. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani "On subsemimodules of semimodules", *Buletinul Academiei de Stiinte a Republicii Moldova, Matematica*, Number 2(63), (2010) Pages: 20–30.
38. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani "Some Remarks On Partitioning Semirings", *Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica*, Vol. 18(1) (2010), Pages: 49–62.
39. Shahabaddin Ebrahimi Atani, Reza Ebrahimi Atani "Very Strong multiplication ideals over a commutative semiring", *Glasnik Matematicki, Glasnik Matematicki*, Vol. 45(65), (2010), Pages: 395 – 406.
40. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "Weak Comultiplication Modules Over a Pullback of Commutative Local Dedekind Domains", *Algebra and Discrete Mathematics*, No. 1. (2009) Pages:1 – 13.
41. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "Comultiplication Modules Over a Pullback of Dedekind Domains", *Czechoslovak Mathematical Journal*, 59(4) (2009), Pages: 1103–1114.
42. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "Secondary representation of semimodules over a commutative semiring", *Quasigroups and related systems*, Issue. 16 (2008), Pages:133–140.
43. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "A Note On Uniformly Primary Submodules", *Novi Sad Journal of Mathematics (NSJOM)*, Vol. 38(2) (2008) Pages: 83–89.
44. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani, Willi Meier "On DPA-Resistive Implementation of FSR-based Stream Ciphers using SABL Logic Styles", *International Journal of Computers, Communications and Control (IJCCC)*, Vol III, 2008, Number 4, Pages: 324–335.
45. Reza Ebrahimi Atani, Willi Meier, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Design and Implementation of DPA Resistive Grain-128 Stream Cipher Based on SABL Logic", *International Journal of Computers, Communications & Control* Vol. III (suppl. issue), 2008, Pages: 293–298.
46. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, Sattar Mirzakuchaki, "Public Key Cryptography using Semi-Group Actions and Semi-Rings", *Journal of Discrete Mathematical Sciences and cryptography*, Vol. 11 (2008), No. 4, Pages: 427–445.
47. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, "Ideal Theory in Commutative Semirings" *Buletinul Academiei de Stiinte a Republicii Moldova, Matematica*, Number 2(57), (2008), Pages: 14–23.
48. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, S. Mirzakuchaki "Public key cryptography based on semi modules over quotient semi rings", *International Mathematical Forum*, 2, 2007, no. 52, Pages: 2561–2570.

## Springer LNCS Book Chapters

1. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Design and Implementation of an Image CoProcessor", *Advances in Image and Signal Processing, Lecture Note in Computer Science* Vol. 5099, Springer (2008), Pages: 498 – 507.
2. Babak Zamanlooy, Vahid Vaghef, Sattar Mirzakuchaki, Ali Bakhtiari, and Reza Ebrahimi Atani, "A Real Time Infrared Imaging System Based on DSP and FPGA ", *Advances in Image and Video Technology, Lecture Note in Computer Science* Vol. 4872, Springer (2007) Pages: 16–23.



## Conference Papers

1. Mehran Pourvahab, Reza Ebrahimi Atani, Laleh Boroumand, "SPKT: Secure Port Knock-Tunneling, an Enhanced Port Security Authentication Mechanism", IEEE Symposium on Computers & Informatics (ISCI 2012), 18 - 20 March 2012, Penang, Malaysia.
2. Nima Karimpour, Reza Ebrahimi Atani, Erfan Aghaei, Ahmad Tahmasivand, Mahsa Rahmani, Mina Moazzam, "CIARP: Crypto Instruction-Aware RISC Processor", IEEE Symposium on Computers & Informatics (ISCI 2012), 18 - 20 March 2012, Penang, Malaysia.
3. Morteza Daneshkar, Reza Ebrahimi Atani, "A Novel Initialization Approach for Solving Permutation Ambiguity of Frequency Domain Blind Source Separation", IEEE Symposium on Computers & Informatics (ISCI 2012), 18 - 20 March 2012, Penang, Malaysia.
4. Reza Moradi Rad, Abdolrahman Attar, Reza Ebrahimi Atani, "A Robust Face Recognition Method Using Edge-Based Features", IEEE Symposium on Computers & Informatics (ISCI 2012), 18 - 20 March 2012, Penang, Malaysia.
5. Anahita Azimi, Mahrokh Maghsoodi, Reza Ebrahimi Atani, "A High Gain UWB common Gate Low-Noise Amplifier", International Conference on Electronics and Communication Engineering (ICECE - 2012), 17 March 2012, Chandigarh, India.
6. Ali Ahmadian Ramaki, Reza Asgari, Reza Ebrahimi Atani, "Ontology-Based Credit Card Fraud Detection", National Congress on Electrical, Computer and Information Technology Engineering, Khayyam Higher Education Institute, Mashhad, Iran, September 15-17, 2012.
7. Mehran Pourvahab, Reza Ebrahimi Atani, Milad Shavandasht, "Port-Knocking with the usage of Web, Internet control message protocol and Tunneling (PWIT)", 6th National Conference Iran's Scientific Society on Command, Control, Communications, Computer and Intelligence (C4I), Nov. 2012, Shahid Beheshti University, Tehran.
8. Ali Ahmadian Ramaki, Shahin Shirmohammadzadeh Sahraei and Reza Ebrahimi Atani, "Security Enforcement with Language-Based Security", Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS 2012), Pages: 26-29.
9. Reza Ebrahimi Atani, Nima Karimpour Darav, Saeedeh Arabani Mostaghim, "A Statistical Test Suite for Windows to Cryptography Purposes", Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS 2012), Pages: 109-113.
10. Seyed Mehrzad Almasi, Hamid Reza Najji, Reza Ebrahimi Atani, "Use of multi-agent system approach for concurrency control of transactions in distributed databases", Third International Conference on Contemporary Issues in Computer and Information Sciences (CICIS 2012), Pages: 426-429.
11. Zahra ghane, Mahrokh Maghsoodi, Reza Ebrahimi Atani, Mehrgan Mahdavi, "A 1-V, 1.3-mW Mixer for MB-OFDM UWB Receivers by 0.18- $\mu$ m CMOS Technology", The Sixth International Symposium on Telecommunications (IST'2012), November 6-8, 2012, Tehran, Iran.
12. Hadi Samiee, Reza Ebrahimi Atani, Hamidreza Amindavar, "A Novel Area-Throughput Optimized Architecture for the AES Algorithm", To appear in the IEEE International Conference on Electronic Devices, Systems & Applications (ICEDSA 2011), 25 - 27 April 2011, Kuala Lumpur, Malaysia.
13. Mehdi Ayat, Reza Ebrahimi Atani, Sattar Mirzakuchaki, Alireza Abdollahi Taromsari, "On Design of Differential Voltage Controlled Oscillators with Single Ended Control Line", IEEE International Conference on Computer Applications & Industrial Electronics, ICCAIE 2010, Kuala Lumpur, Malaysia, 5 - 7 December 2010, Pages: 397-402.
14. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Functions", To appear in the proceeding of the 6th Iranian Conference on Machine Vision and Image Processing (MVIP 2010), October. 2010, Isfahan, Iran.
15. Yadollah Zamanidoost, Sattar Mirzakuchaki, Reza Ebrahimi Atani, Zhinoos Razavi Hesabi, Mehdi Ayat, "A Novel 3D Wavelet-Based Method for Blind Digital Video Watermarking", IEEE International Symposium on Industrial Electronics and Applications, ISIEA 2010, Penang, Malaysia, 3 - 5 October 2010, Page(s): 186 - 189.

16. Mehdi Ayat, Reza Ebrahimi Atani, Sattar Mirzakuchaki, Yadollah Zamanidoost, "Design and Simulation of a CMOS DLL-Based Frequency Multiplier", IEEE International Symposium on Industrial Electronics and Applications, ISIEA 2010, Penang, Malaysia, 3 – 5 October 2010, Page(s): 450–455.
17. Mehdi Ayat, Behnam Babaei, Reza Ebrahimi Atani, Babak Zamanlooy, Sattar Mirzakuchaki, "Design of A 100 MHz - 1.66 GHz, 0.13um CMOS Phase Locked Loop", IEEE International Conference on Electronic Devices, Systems & Applications (ICEDSA2010), 11 – 13 April 2010, Kuala Lumpur, Malaysia, Pages 154–158.
18. Sakineh Aghighi, Reza Ebrahimi Atani "Averaged Value Analysis of 24-Pulse Rectifiers for Aerospace Applications", IEEE International Conference on Electronic Devices, Systems & Applications (ICEDSA 2010), 11 – 13 April 2010, Kuala Lumpur, Malaysia, Pages 212 – 217.
19. Mohamadamin Amiri, Mojdeh Mahdavi, Reza Ebrahimi Atani, Sattar Mirzakuchaki "QCA Implementation of Serpent Block Cipher", Advances in Circuits, Electronics and Micro-electronics (CENICS'09), October 11-16, 2009, Sliema, Malta, Pages: 16 – 19.
20. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Alamout: A new Synchronous stream cipher with Authentication", WirelessVITAE'09, May 17-20, 2009, Aalborg, Denmark, Pages: 886 – 890.
21. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Low Cost Implementation of Pomaranch S-Boxes", WirelessVITAE'09, May 17-20, 2009, Aalborg, Denmark, Pages: 875 – 879.
22. Sakineh Aghighi, Alfred Baghramian, Reza Ebrahimi Atani "Averaged Value Analysis of 18-Pulse Rectifiers for Aerospace Applications", IEEE International Symposium on Industrial Electronics (ISIE 2009), July 5 - 8, 2009, Seoul, Korea. Pages: 1498 – 1503.
23. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Design and Simulation of a DPA Resistive Circuit for Trivium Stream Cipher Based on SABL Logic Styles", ICMSAO'09, Jan. 20-22 2009 , Sharjah, U.A.I..
24. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani "Design and simulation of A DPA Resistive Circuit for Trivium Stream Cipher Based on WDDL logic Styles", ICMSAO'09, Jan. 20-22 2009 , Sharjah, U.A.I..
25. Reza Ebrahimi Atani, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani, Willi Meier "Design and Simulation of a DPA Resistive Circuit for Trivium Stream Cipher Based on SABL Logic Styles", MIXDES'08, Poznan, 19-21 June 2008, p.p. 203 – 208.
26. Babak Zamanlooy, Hamidreza Chamani Takaldani, Amir Moosavienia, Khalil Monfaredi and Reza Ebrahimi Atani "Design and Implementation of a Stable Platform Digital Controller Based on DSP", International Conference on Signals and Electronic Systems, (ICSES '08), (2008), Krakow, Poland, Pages: 453 – 456.
27. Reza Ebrahimi Atani, Mehdi Baboli, Sattar Mirzakuchaki, Shahabaddin Ebrahimi Atani, and Babak Zamanlooy, "Design and Implementation of a 118 MHz 2D DCT Processor", IEEE International Symposium on Industrial Electronics (ISIE 2008), 30 June-2 July, 2008, Cambridge, UK, Pages: 1076 – 1081.
28. R. Ebrahimi Atani, Mehdi Baboli, and S. Mirzakuchaki, "Analysis and Implementation of WiMAX security system ", EHAC 2008, February 20-22, 2008, Cambridge, UK, Pages Pages: 107–110.
29. Farshid Samii Amlashi, Adib Abrishamifar, and Reza Ebrahimi Atani, "Jitter Peaking Investigation in Charge Pump Based Clock and Data Recovery Circuits", Africon 2007, 26 - 28 September 2007, Namibia, Pages: 1 – 6.
30. M. Amiri , R. Ebrahimi Atani, S. Mirzakuchaki, and M. Mahdavi " Design and Implementation of A 50MHZ DXT Coprocessor " 10th Euromicro Conference on Digital System Design Architectures, Methods and Tools (DSD 2007), August 29 - 31, Lubeck - Germany, 2007, Pages: 43-50.

31. R. Ebrahimi Atani, S. Mirzakuchaki, Farshid Sanii Anlashi, and M. Nasrollahzadeh, "Design and Implementation of a 157 MHz DA-Based DXT CoProcessor", IEEEGCC 2007, Manamma, Bahrain, 11-14 November 2007.

### **Technical Reports**

1. Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, Sattar Mirzakuchaki "A Novel Public Key Crypto System Based on Semi-modules over Quotient Semi-rings", eprint Archive, 2007/391 .

### **Advisory for Post Graduate Programs**

#### **Current MSc. Students**

Farhad Farrokhpanah 2011  
Somayeh Mirzaei 2010  
Mohammad Sharifi 2009  
Mostafa Rahmanpour 2009  
Sara Salehi Mahboub 2009  
Faraz Ghasempour 2009  
Mohammad Nezadeh 2009  
Ali Deghati 2009  
Saeed Mehmandoust 2009  
Hossein Jadidoleslami 2009  
Majid Emadi 2009  
Maryam Pirouz 2009  
Zahra Nourizadeh 2009  
Farzad Tavakkoli 2009

#### **Program Committee**

The 10th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2013), Yazd University, September 14-15 2013, Yazd, Iran.

The 9th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2012), Tabriz University, September 14-15 2012, Tabriz, Iran.

International Conference on Advanced Information Technologies and Applications (ICAITA-2012), 28-29 Dec. Dubai, UAE.

International Workshop on Education Engineering and Economics (IW3E 2011), Zhengzhou, China Aug 8-10th, 2011.

The Second International Conference on Computer Science, Engineering and Applications (ICCSEA 2012), May 25-27, 2012, New Delhi, India.

International workshop on Foundations of Computer Science & Technology (CST-2013), February 18 - 20, 2013, Bangalore, India

International Conference on Foundations of Computer Science & Technology (FCST-2012), 14-15 July, Chennai, India.

Interdisciplinary Conference on Art, Language & Technology (ICALT2012), Mashhad, Iran.

The 9th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2012), University of Tabriz, September 14-15, 2012, Tabriz, Iran.

2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC 2011), Aug. 8-10, 2011, Zhenzhzhou, China.

International workshop on Cryptography and Information Security (CRYPIS-2012), October 26 28, 2012, Venue : Avinashilingam University, Coimbatore, India.

The Second International Conference on Computational Science, Engineering and Information Technology (CCSEIT-2012), Venue: Avinashilingam University, October 26 28, Coimbatore, India.

International workshop on Signal Image Processing and Multimedia (SIPM-2012), 14-15 July, Chennai, India.

First International Conference on Signal, Image Processing and Pattern Recognition (SPPR 2012), May 24-26, Delhi, India.

The International Conference on e-Learning and Knowledge Management Technology ( ICEKMT 2011 ), July. 8-9, 2011, Kuala Lumpur, Malaysia. <http://www.icekm.com/index.php>

First International Conference on Signal, Image Processing and Pattern Recognition (SPPR 2012), 2nd International Conference on Management Science and Artificial Intelligence (MSAI 2011), Aug. 8-10, 2011, DengFeng, China.

The 8th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2011), Ferdowsi University of Mashhad, September 14-15 2011, Mashhad, Iran.

3rd National Conference on Computer Engineering and Information Engineering (CEIT 2011), 17 February, 2011, Hamedan, Iran.

The 2nd International Conference on Management Science and Artificial Intelligence (MSAI 2011), Aug. 8-10, 2011, DengFeng, China.

The 8th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC 2011), Ferdowsi University of Mashhad, September 14-15 2011, Mashhad, Iran.

## **I have reviewed articles for**

### **Journal refereeing:**

IEEE Transactions on Circuits and Systems for Video Technology 2009/2010/2011

Journal of Systems and Software

Journal of Nature Science and Sustainable Technology

IET Information Security

Analele Stiintifice ale Universitatii Ovidius Constanta, Seria Matematica

Security and Communication Networks

International Journal on Cryptography and Information Security - IJCIS

International Journal in Foundations of Computer Science & Technology - IJFCST

International Journal on Bioinformatics & Biosciences - IJBB

International Journal on Organic Electronics- IJOE

International Journal of Programming Languages and Applications- IJPLA

International Journal of Advanced Information Technology - IJAIT

International Journal of Network Security

Journal of Technical-Engineering, Islamic Azad University Mashhad Branch  
Biannual journal, Signal and Data Processing  
Italian Journal of Pure and Applied Mathematics.

**Conference refereeing:**

IEEE 69th Vehicular Technology Conference, (VTC2009 - Fall)  
IEEE International Conference on Electronic Devices, Systems & Applications, (ICEDSA 2010, ICEDSA 2011)  
IEEE Symposium on Industrial Electronics & Applications, (ISIEA 2010, ISIEA 2011)  
IEEE International Conference on Computer Applications & Industrial Electronics, (ICCAIE 2010)  
IEEE International Conference on Scientific & Social Science Research, (CSSR 2010)  
IEEE International Conference on Open Systems, (ICOS 2010)  
36th Annual Conference of the IEEE Industrial Electronics Society, (IECON 2010)  
7th International ISC Conference on Information Security and Cryptology (ISCISC 2010)  
IEEE Applied Power Electronics Colloquium (IEEE-IAPEC 2011)  
IEEE International Symposium on Computers & Informatics, (ISCI 2011)  
IEEE International Symposium on Humanities, Science and Engineering (SHUSER 2011)  
IEEE International Conference on Business, Engineering and Industrial Applications (ICBEIA 2011)  
IEEE International Conference on Signal & Image Processing Applications (ICSIPA 2011)  
National Conference On information And Communication Security, (CICS 2010)  
3rd National Conference on Computer Engineering and Information Engineering (CEIT 2011)  
The International Conference on Informatics Engineering & Information Science (ICIEIS2011)  
The International Conference on Digital Information & Communication Technology & its Applications (DICTAP 2011)  
The International Conference on Digital Information Processing & Communications (ICDIPC 2011)  
The International Conference on Electronic Technologies & Digital Computing (ETDC2011)  
The First International Conference on e-Technologies and Networks for Development (ICeND2011)  
The International Conference on Digital Enterprise and Information Systems (DEIS 2011)  
The 2nd International Conference on Software Engineering and Computer Systems (ICSECS 2011)  
The 19th Iranian Conference on Electrical Engineering (ICEE 2011)