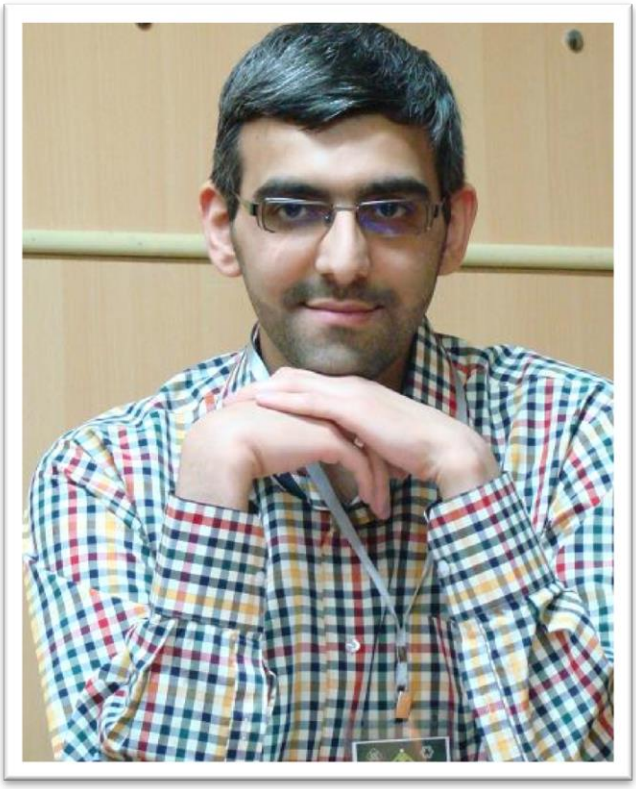

Mohammad Ehdaie

Curriculum Vitae

About

Titles and Positions

- Cryptography & Security Expert
- Electrical Engineering PhD @ K.N.Toosi University
- Lecturer @ Sharif University of Technology
- Product Manager @ PKI Company
- Managing Editor @ Sama Magazine

Small Snapshot

Mohammad Ehdaie is a Product Manager at PKI Company. He likes to research, to create, and to present. He likes to plan, to generate ideas, to lead a team, and to meet the mission.

He is interested in designing algorithms and protocols. He started programming when he was 7. He well knows how to make creative solutions for problems.

His intelligence brought to him a dozen of scientific achievements, such as ranking 39-th amongst 450,000 participants in national university entrance exam and studying in the best university of Iran.

Since he is passionate about teaching and presenting, he started teaching at Sharif university when he was a MSc student. He showed a great ability as a teacher and taught programming to 2,000+ talented students.

When he was a PhD student, he organized a group of motivated students for scientific activities. During 2 years, he organized 4 workshops and conferences at international level with 500+ participants in total. Those events were a clear example of planning, team-working, and leadership.

Now, he leads Mobile Signature Service, a national project for MCI (main mobile operator in Iran). He well knows how to manage the things, to prioritize the work-load, and to present to C-level managers.

He still seeks better opportunities to utilize his skills in a larger scale. Mohammad Ehdaie is alive to not stop.

Contacts and Links

- Web: www.ehdaie.ir
- e-mail: mohammad@ehdaie.ir
- LinkedIn
- Google Scholar
- Research Gate

Contents

Work Record

Product Manager

PKI Company

Dec. 2014 - Present

Managing Editor

Sama Magazine

Sep. 2013 - Present

Project Manager

PKI Company

Dec. 2012 - Present

Senior Product Expert

PKI Company

Nov. 2013 - Dec. 2014

Research and Develop

Rastafan (Fanamoj)

Jun. 2005 - Nov. 2008

Code Developer

Rastafan (Fanamoj)

Jun. 2005 - Nov. 2008

Research Record

IoT Security	**Self-Study** Jan. 2015 - Present
User Authentication Methods	**Self-Study** Dec. 2013 - Present
Wireless Networks Security	**KTH, Sweden** Jan. 2012 - Sep. 2012
Key Management in WSNs	**K.N.Toosi University of Technology** Sep. 2008 - Feb. 2014
Secret Sharing	**Sharif University of Technology** Nov. 2005–Sep. 2008
Boolean Functions	**Sharif University of Technology** Dec. 2005–Jul. 2006

Teaching Record

C Programming

Sharif University of Technology
Lecturer – Since Jan. 2009

Pascal Programming

Sharif University of Technology
Lecturer; Since Jan. 2006

Probability and Statistics

Sharif University of Technology
Teaching Assistant; Sep. 2003–Jan. 2004

Pascal Programming

Sharif University of Technology
Teaching Assistant; Sep. 2003–Dec. 2005

Education Record

PhD

Electrical Engineering; Communications Systems

K.N.Toosi University of Technology; 2008-2014

MSc

Electrical Engineering; Cryptology

Sharif University of Technology; 2005-2007

BSc

Electrical Engineering; Communications

Sharif University of Technology; 2001-2005

Activities and Memberships

Book Referee in Programming Area	IEEE Membership	Iranian Society of Cryptography Associate Membership
Head of Executive Council Iranian Society of Cryptography Student Branchin KNTU	Student Guild Membership Sharif University of Technology	Reviewing papers ISCISC Conference
Executive Committee Member ISCISC 2010	National Elites Foundation Membership	Head of Secret Sharing Research Group Sharif University of Technology
Advising MSc. Students		Examiner in BSc. Defense Session

Skills

Selected Skills

Management	(10/10)
Presentation	(10/10)
Security	(9/10)
Programming	(9/10)

Languages

Farsi (Native)	(10/10)
Written English	(9/10)
Oral English	(6/10)
Arabic	(3/10)

Management Skills

Team Leadership	(10/10)
Team Management	(10/10)
Project Management	(9/10)
Product Management	(9/10)
SWOT Analysis	(7/10)
Data Envelopment Analysis	(7/10)

Presentation Skills

Technical Presentation	(10/10)
Product Presentation	(10/10)

Network Security	Wireless Sensor Networks Security	(9/10)
	Ad-hoc Networks Security	(8/10)
	Distributed Networks Security	(8/10)
	Key Management Schemes	(10/10)
	Key Distribution Protocols	(10/10)
	Secret Sharing Schemes	(9/10)
User Authentication	2-Factor Authentication	(9/10)
	mobile PKI	(10/10)
	e-Signature as a Services	(10/10)
	Authentication as a Services	(9/10)
Computer Skills	MATLAB	(8/10)
	LATEX	(7/10)
	Microsoft Office	(9/10)
	C Programming	(9/10)
	Delphi Programming	(10/10)
Basic Sciences Skills	Probability Theory	(10/10)
	Combinatorial Theory	(7/10)
	Information Theory	(7/10)
	Data Clustering	(7/10)

Invited Talks

A New Audio and Visual Secret Sharing Scheme

Monthly Seminar, Iranian Society of Cryptology

February 2008

Secret Sharing: a survey and open problems

Selected Areas in Cryptology-I workshop, KNTU

November 2010

Secret Sharing: a survey and open problems

Selected Areas in Cryptology-II workshop, MAUT

December 2010

Key Distribution in WSNs

Sensor and Ad-hoc Networks Security workshop, KNTU

April 2011

Key Distribution in WSNs

Sensor and Ad-hoc Networks Security workshop, KNTU

April 2011

Publications

Key Splitting: Making Random Key Distribution Schemes Resistant against Node Capture

Mohammad Ehdaie, Nikos Alexiou, Mahmoud Ahmadian, Mohammad Reza Aref, Panos Papadimitratos

Security and Communications Networks, John Wiley, 2014(2)

Key Splitting for Random Key Distribution Schemes

Mohammad Ehdaie, Nikos Alexiou, Mahmoud Ahmadian, Mohammad Reza Aref, Panos Papadimitratos

IEEE NPsec 2012

Secure Broadcasting and Unicasting in WSNs

Hassan Nasiraie, Jamshid Bagherzadeh, Mohammad Ehdaie

8th International ISC conference, 2011

A Novel Secret Sharing Scheme from Audio Perspective

Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref

IST 2008, I.R.Iran (Selected for Journal publication)

Some New Issues on Secret Sharing Schemes

Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref

ICT 2008, Russia

A New Method for Visual Secret Sharing

Hamed Firouzi, Mohammad Ehdaie, Mohammad Reza Aref

IST 2008, I.R.Iran

A New Threshold Audio Secret Sharing Scheme

Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref

WEWoRC 2007, Ruhr Univ., Bochum, Germany

New Threshold Audio and Visual Secret Sharing Schemes

Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref

In Progress

Information Theoretical View to an Audio Secret Sharing Scheme

Mohammad Ehdaie, Taraneh Eghlidos, Mohammad Reza Aref

In Progress

Random Key Distribution against Sybil Attack

Nikos Alexiou, Mohammad Ehdaie, Panos Papadimitratos

In Progress

2-D Hash Chain to Make RKD Schemes Resistant

Mohammad Ehdaie, Nikos Alexiou, Mahmoud Ahmadian, Mohammad Reza Aref, Panos Papadimitratos

In Progress

Success Stories

Scientific Titles

- First Ranking in Scientific Competition, Regional Competition, 3rd grade, Elementary School, Region 1, Ahvaz, 1991.
- First Ranking in Scientific Competition, Regional and State Competition, 5th grade, Elementary School, Khouzestan , 1993.
- First Ranking in Scientific Competition, Regional and State Competition, 1st grade, Guidance School, Khouzestan , 1994.
- 4th Ranking in Scientific Competition, National Competition, 1st grade, Guidance School, 1994.
- 3rd Ranking in 'AyandeSazan' Competition, City Competition, 1st grade, Guidance School, Ahvaz, 1994.
- 5th Ranking in 'AyandeSazan' Competition, State Competition, 1st grade, Guidance School, Khouzestam, 1994.
- -101st Ranking in 'AyandeSazan' Competition, National Competition, 1st grade, Guidance School, 1994.
- 1st Ranking in 'AyandeSazan' Competition, City Competition, 2nd grade, Guidance School, Tehran, 1995.
- 11th Ranking in 'AyandeSazan' Competition, State Competition, 2nd grade, Guidance School, Tehran, 1995.
- 91st Ranking in 'AyandeSazan' Competition, National Competition, 2nd grade, Guidance School, 1995.
- 16th Ranking in 'AyandeSazan' Competition, National Competition, 3rd grade, Guidance School, 1996.
- 39th Ranking, National University Entrance Examination, 2001.
- Admission in PhD. course of Amirkabir University of Technology, 2007.
- Invited to Interview stage for PhD. course of IUST, 2008.
- Admission in PhD. course of Amirkabir University of Technology, 2008.

Programming Projects

- A Multimedia Program for Learning SPSS (a Statistics Program).
- Software of Computing and Plotting Some Electromagnetic Parameters.
- Implementation of RSA Encryption System.
- Implementation of CBC-DES and 3-DES Encryption Systems.
- Implementation of SHA-1 Message Digest Algorithm.
- Software of Preparing Report Cards for School.
- Administrator Software of a Communication Project, with Serial Port Interface and SQL-Server Database.
- Insurance Software Package, According to the Iranian Central Insurance Laws.

- Personal and Commercial Accounting Program.
- 'Omre' Lottery Program for Sharif University of Technology.
- Football Game
- Intelligent Motoring
- 3D Motoring
- Artificial Intelligence Based X-O.

Teaching

I started teaching at Sharif university as a formal lecturer when I was a MSc. student. Based on feedback from students, my score was always around 3.8 out of 4. My outstanding scores encouraged faculty to assign me more groups and courses.

It is my pleasure to teach programming to 2,000+ talented students during 14 semesters.

Sama Magazine

Sama is an IT security magazine for IT professionals in Iran. It covers a broad range of information and communication security issues including but not limited to: PKI, SOC, ISMS, VPN, UTM, WAF, IPS, IDS, Network Security, Security issues in office automation, Business Data Breaches, Web Security, Mobile Security, and so on. We started this magazine at our company with a small, but effective and motivated group. The first issue was prepared within 45 days from the start-up. The wonderful output was admired by CEO and Board of Directors.

I, as a Managing Editor, was responsible for almost everything in the flow: from preparing appreciate material to reviewing received papers, writing some papers in my expertized field, translating some others from reliable resources, and preparing questions for interview with governmental managers and academic experts. I also contributed in titling and designing issues.

Sama Magazine is a real example of a '0 to 100' project and illustrates my ability to work independently or as a leader of a group.

Mobile Signature Service Project

MSS is a national project, aims to digitally authenticate every citizen based on his/her legal digital signature. The signature is generated in the user SIM-card, so it is mobile and user-friendly. In the other hand, it is provided to organizations as a service. It is possible for any Application Provider (AP) to authenticate his/her usersvia a standard web service call.

This project involves close work with Mobile Operator from one side, as well as an organization like a bank. I, as the project manager, am responsible with technical issues of the project, also with handling tasks at the C-level, plus presenting the system to customers and advertising and business issues.

Now, after our two years persistence in developing the project, it is accepted as a high-priority project by MCI (main mobile operator of Iran). More wonderfully, it is to be launched in one of the innovative banks in country.

Elecomp 2013 Exhibition

Elecomp is the most important exhibition in the field of Electronics and Computers in Iran. My

company attended in this fair every year. In 2013, the company decided to organize some technical workshops during the exhibition days and I was selected as the workshops manager.

I organized 16 workshops during four days, four 45-minute workshops a day. The workshops were presented by our technical staffs, including me. They were held with high-level discipline and attracted a lot of audiences to our pavilion.

Because of the workshops, Elecomp 2013 turned to one of our successful and memorable exhibitions.

Organizing Events

Iranian Society of Cryptography Student Branch in K.N.Toosi University was one of the most admirable student groups between 2009 and 2011.A group of 25 active and motivated students who decided to do works in a different manner. They believed they can make impossible things possible.As a scientific student group, they were organizing seminars and workshops for interested people, but not like others. They didn't want to hold a workshop, at a low scientific level, for a few number of their colleagues, without any output.

The first workshop they organized was entitled 'Selected Areas in Cryptology' and covered a broad range of fields in data security, including Block Ciphers, Stream Ciphers, Asymmetric Cryptography, Digital Signature, Hash Functions, e-Voting,Secret Sharing, Steganography and Watermarking. These topics were taught by 8 professionals during 2 days. Around 60 young researchers from most of universities attended the workshop. Even, we had some participants from other cities, who drove 4 hours to take part the workshop. Even more, there were many applicants from big companies who asked to attend the workshop such that we were out of space. The workshop was held with very high regularity and discipline. The event was admired by Professor Aref, the chief for ISC.

We received a lot of requests to repeat the workshop for those who failed to attend. So, we organized another workshop with the same topics for them. This time, we moved to another location to be enough for our 110 participants. Out third workshop was expertized in Watermarking and Steganography and was held a few months after our second one. In another word, we organized 3 workshops only during 6 months, which was outstanding.

That wasn't the end. We still was motivated to do something better. Thus, we started organizing an International event. For our new workshop, we decided to focus on 'Ad-hoc and Sensor Networks Security'. We invited two professional researchers who were amongst the bests in world:

1- Keith Martin, full professor at Royal Holloway, university of London. Everyone in thefield of Key Management knows him.

2- Panos Papadimitratos, Associate Professor at KTH, Stockholm, who has a great research record specially in the field of routing protocols in Ad-hoc networks. His famous paper was cited by 1600+.

We worked 6 months, days and nights, to organize a brilliant event, as Keith noted in the final, or as Panos admired us. We had to handle everything, from inviting other researchers to talk, to book a ticket and a 5-star hotel for Keith and Panos, organizing tours for our honorable guests to visit Iran tourist attractions, organizing dinner ceremonies, and everything you think. We were surprised when 250 participants from Tehran and other cities, including students, faculty members and researchers from related companies, booked to attend the workshop.

This two-year experience as the head of group was one of my best memories and a clear example of team working.