



# Mahdi Daghmehchi Firoozjaei

*Resume (December 27, 2017)*

---

*Address*            Sungkyunkwan University, Suwon 440-746, Republic of Korea  
*Phone*             (+82) 31-299-4104  
*E-Mail*             [mdaghmechi@skku.edu](mailto:mdaghmechi@skku.edu)  
*WWW*               <http://seclab.skku.edu/people/mahdi/>

## **EDUCATION**

---

**Ph.D in Electrical and Computer Engineering** 2014-2017

*Sungkyunkwan University, Suwon, Republic of Korea*

Thesis: A Study on Privacy-preserving Systems for Network Services  
(Examiners: Prof. Tai-Myoung Chung and Prof. Jaehoon (Paul) Jeong)  
Advisor: Prof. Hyoungshick Kim

**M.Sc. Telecommunication-Cryptology** 2002-2005

*Imam Hossein Comprehensive University, Tehran, Iran*

Thesis: "Review Security Weaknesses of IPSec and Suggestions for Improving Them"  
Advisors: M. Saleh Esfahani (Imam Hossein Comprehensive University) / A. Yazdian Varjani (Tarbiat Modares University)

**B.Sc. Telecommunication Engineering** 1996-2000

*Scientific-Applied Faculty of Post and Telecommunication, Tehran, Iran*

Thesis: "Designing and Implementing an Announcement System for Public Phone Systems"

## **RESEARCH INTERESTS**

---

- Cryptography; Network Security
- Users' Privacy Preserving in the Cellular Networks
- Secure Emergency Messaging Systems & False Requests Detecting
- Network Functions Virtualization- NFV; Security Issues
- Geo-encryption; Secure Location Based Services

## APPOINTMENTS

---

**Telecommunication Company of Mazahdaran-TCM, Babol, Iran** 2006-2014  
*Engineer- Management of Maintenance and Supporting*

- 2011-2014: Maintenance Department of Data Transmission Networks
- 2010-2011: RF Planning and Optimization Department of Cellular Network
- 2006-2010: Operational Analyzing of Telephone Exchanges

**Part Time Lecturer of Information and Communication Technology** 2006-2013  
*Mazandaran University of Science and Technology, Babol, Iran (2013)*

- Teaching course on Information Security

*Allameh Amini High Education Institute, Bahnamir, Iran (2012-2013)*

- Teaching courses on Signals and Systems Processing and Communication Transmission Systems

*Shomal University, Amol, Iran (2006-2012)*

- Teaching courses on Analogue Communication Systems, Digital Communication Systems, and Computer Programming Language

## REFEREED PUBLICATIONS

---

12. Mahdi Daghmehchi Firoozjaei, Sangmin Lee, and Hyoungshick Kim, “[O<sup>2</sup>TR: Offline Off-the-Record \(OTR\) Messaging](#)”, *WISA: The 18th World Conference on Information Security Applications 2017* , Jeju Island, Korea (2017).
11. Mahdi Daghmehchi Firoozjaei, Jaehoon (Paul) Jeong, Hoon Ko, and Hyoungshick Kim, “[Security Challenges with Network Functions Virtualization](#)”, *ELSEVIER- Future Generation Computer Systems 67 (Feb 2017)* , 315-324 (2017).
10. Mahdi Daghmehchi Firoozjaei, Jaegwan Yu, Hyoungkee Choi, and Hyoungshick Kim, “[Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks](#)”, *ELSEVIER- Computer Communications 98 (Jan 2017)* , 11-19 (2017).
9. Mahdi Daghmehchi Firoozjaei, Minchang Kim, and Hyoungshick Kim, “How Practical is OTR?”, *CISC-S'16: Conference on Information Security and Cryptography 2016* , Busan, Korea (2016).
8. Mahdi Daghmehchi Firoozjaei, Jaewoo Park, and Hyoungshick Kim, “[Detecting False Emergency Requests Using Callers' Reporting Behaviors and Locations](#)”, *DC2-2016: The 3rd International Workshop on Device Centric in conjunction with IEEE AINA* , Crans-Montana, Switzerland (2016).
7. Jinyong Kim, Mahdi Daghmehchi, Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park, “[SDN-based Security Services using Interface to Network Security Functions](#)”, *ICTC: The 6th International Conference on ICT Convergence* , Jeju Island, Korea (2015).
6. Mahdi Daghmehchi Firoozjaei, Jaegwan Yu, and Hyoungshick Kim, “[Privacy Preserving Nearest Neighbor Search based on Topologies in Cellular Networks](#)”, *DC2: The 2nd Workshop on Device Centric Cloud held in conjunction with IEEE AINA* , Gwangju, Korea (2015). (Selected as “best paper”)
5. Mahdi Daghmehchi Firoozjaei and Javad Vahidi, “[Implementing Geo-encryption in GSM cellular Network](#)”, *COMM 2012: 9th International Conference on Communication* , Bucharest, Romania (2012).
4. Mahdi Daghmehchi Firoozjaei and Ali Yazdian, “Evaluating Geo-encryption application in a cellular network, case study using GSM”, *ISCEE 2011: 14th Iranian Student Conference on Electrical Engineering (in Persian)*, Kermanshah, Iran (2011).
3. Mahdi Daghmehchi Firoozjaei and Ali Yazdian, “[Improving IPSec Security Weaknesses in the decryption key forgery situation](#)”, *16th Annual Computer Society of Iran Computer Conference (in Persian)*, Tehran, Iran (2011).
2. Mahdi Daghmehchi Firoozjaei, “[Using MS location information in GSM encryption key generation, Study case: Geo-Encryption algorithm](#)”, *National Conference on Information and Communication Security (in Persian)*, Ahvaz, Iran (2010).
1. Mahdi Daghmehchi Firoozjaei, “Comparison between VPN solutions: MPLS, SSL, and IPSec”, *7th Computer Engineering Student Conference (in Persian)*, Tehran, Iran (2005).

## PROFESSIONAL SOCIETIES AND SERVICE

---

- Reviewer of:
  - Telecommunication Systems Journal- Springer
  - Computer & Electrical Engineering Journal- ELSEVIER
  - COMM2014, 10th International Conference on Communications
- Membership:
  - Iranian Society of Cryptology- ISC

## AWARDS

---

- **The 2nd Prize for the Superior Research Award**, College of Information and Communication Engineering, Sungkyunkwan University, August 3th 2017
- **The best paper award**, DC2: The 2nd Workshop on Device Centric Cloud, 2015
- **The SKKU Scholarship for outstanding international students**, Sungkyunkwan University, 2014-2018

## TEACHING

---

- Fall 2013: **Information Security**  
Computer and Information Technology Group, Mazandaran University of Science and Technology
- Spring 2011 - Fall 2013: **Communication Transmission Systems**  
Allameh Amini High Education Institute
- Spring 2011: **Signals and Systems Processing**  
Allameh Amini High Education Institute
- Spring 2008 - Fall 2012: **Digital Communication Systems**  
Department of Electrical & Electronic Engineering, Shomal University
- Spring 2006 - Spring 2012: **Analog Communication Systems**  
Department of Electrical & Electronic Engineering, Shomal University
- Spring & Fall 2006: **C Programming Language**  
Department of Electrical & Electronic Engineering, Shomal University

## TECHNICAL/SPECIAL SKILLS

---

- **Programming:** C/C++, Python, and Pascal
- **Simulation and Math package:** Matlab
- **Languages:** English, Arabic, and Persian (native language)

## REFERENCES

---

- **Hyoungshick Kim**

Assistant Professor,  
Department of Computer Science and Engineering,  
College of Information and Communication Engineering,  
Sungkyunkwan University (SKKU),  
Suwon, Gyeonggi-Do, 440-746,  
Republic of Korea,  
Tel: +82 31-299-4324,  
E-mail: [hyoung@skku.edu](mailto:hyoung@skku.edu),  
Personal Homepage: <http://seclab.skku.edu/people/hyoungshick-kim/>

- **Jaehoon (Paul) Jeong**

Assistant Professor,  
Department of Software,  
College of Information and Communication Engineering,  
Sungkyunkwan University (SKKU),  
Suwon, Gyeonggi-Do, 440-746,  
Republic of Korea  
Tel: +82 31-299-4957  
E-mail: [pauljeong@skku.edu](mailto:pauljeong@skku.edu)  
Personal Homepage: <http://iotlab.skku.edu/people-jaehoon-jeong.php>