

# Mahdi Daghmehchi Firoozjaei

Curriculum Vitae (Dec. 12, 2017)

---



## Personal Information:

Date of birth: May 22, 1977  
Address: Sungkyunkwan University, Suwon 440-746,  
Republic of Korea  
Phone: (+82) 31-299-4104  
Email: [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. in Telecommunication- Cryptology** 2002-2005

Imam Hossein Comprehensive University, Tehran, Iran

Thesis: A Study on Security Weaknesses of IPSec and Mitigation Suggestions

Advisors: Prof. A. Yazdian Varjani (Tarbiat Modares University) and

Prof. M. Saleh Esfahani (Imam Hossein Comprehensive University)

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

Scientific-applied Faculty of Post and Telecommunication, Tehran, Iran

## ADWARDS AND GRANTS

---

- **The 2nd Prize for the Superior Research Award**, College of Information and Communication Engineering, Sungkyunkwan University, August 3th 2017.
- **The Best Paper Award**, DC2-2015: The 2<sup>nd</sup> International Workshop on Device Centric Cloud, 2015.
- **The SKKU Scholarship for Outstanding International Students**, Sungkyunkwan University, 2014-2018

## APPOINTMENTS

---

Telecommunication Company of Mazandaran- TCM, Babol, Iran 2006-2014

Engineer in the Department of Network Maintenance and Supporting Management

## SELECTED REFERRED PUBLICATIONS

---

- **Mahdi Daghmehchi Firoozjaei**, Sangmin Lee, and Hyounghshick Kim, “O2TR: Offline Off-the-Record (OTR) Messaging”, *WISA: The 18<sup>th</sup> World Conference on Information Security Applications 2017*, Jeju Island, Korea (2017).
- **Mahdi Daghmehchi Firoozjaei**, Jaehoon (Paul) Jeong, Hoon Ko, and Hyounghshick Kim, “Security Challenges with Network Functions Virtualization”, *ELSEVIER- Future Generation Computer Systems 67 (Feb 2017)*, 315-324 (2017).
- **Mahdi Daghmehchi Firoozjaei**, Jaegwan Yu, Hyounghshick Choi, and Hyounghshick Kim, “Privacy-Preserving Nearest Neighbor Queries Using Geographical Features of Cellular Networks”, *ELSEVIER- Computer Communications 98 (Jan 2017)*, 11-19 (2017).
- **Mahdi Daghmehchi Firoozjaei**, Jaewoo Park, and Hyounghshick Kim, “Detecting False Emergency Requests Using Callers’ Reporting Behaviors and Locations”, *DC2-2016: The 3<sup>rd</sup> International Workshop on Device Centric Cloud in conjunction with IEEE AINA*, Crans-Montana, Switzerland (2016).
- Jinyong Kim, **Mahdi Daghmehchi**, Jaehoon (Paul) Jeong, Hyounghshick Kim, and Jung-Soo Park, “SDN-based Security Services using Interface to Network Security Functions”, *ICTC: The 6<sup>th</sup> International Conference on ICT Convergence*, Jeju Island, Korea (2015).
- **Mahdi Daghmehchi Firoozjaei**, Jaegwan Yu, and Hyounghshick Kim, “Privacy Preserving Nearest Neighbor Search based on Topologies in Cellular Networks”, *DC2-2015: The 2<sup>nd</sup> International Workshop on Device Centric Cloud in conjunction with IEEE AINA*, Gwangju, Korea (2015). (Selected as “best paper”)
- **Mahdi Daghmehchi Firoozjaei** and Javad Vahidi, “Implementing Geo-encryption in GSM cellular Network”, *COMM 2012: 9<sup>th</sup> International Conference on Communication*, Bucharest, Romania (2012).
- **Mahdi Daghmehchi Firoozjaei** and Ali Yazdian, “Evaluating Geo-encryption application in a cellular network, case study using GSM”, *ISCEE 2011: 14<sup>th</sup> Iranian Student Conference on Electrical Engineering (in Persian)*, Kermanshah, Iran (2011).
- **Mahdi Daghmehchi Firoozjaei** and Ali Yazdian, “Improving IPSec Security Weaknesses in the decryption key forgery situation”, *16<sup>th</sup> Annual Computer Society of Iran Computer Conference (in Persian)*, Tehran, Iran (2011).

## RESEARCH INTERESTS

---

- Cryptography; Network and Information Security
- Privacy Preserving in the Cellular Network Communication
- Secure Emergency Messaging; False Request Detecting
- Network Functions Virtualization- NFV; Security Issues
- Geo-Encryption; Secure Location-Based Services (LBSes)

## PROFESSIONAL SOCIETIES AND SERVICE

---

### Reviewer of:

- Telecommunication System Journal- Springer
- Computer & Electrical Engineering Journal- ELSEVIER
- COMM2014, 10<sup>th</sup> International Conference on Communications

### Membership:

- Iranian Society of Cryptology- ISC

## TECHNICAL/SPECIAL SKILLS

---

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

## REFERENCES

---

- **Hyounghick Kim**

Assistance 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                      Email: [hyoung@skku.edu](mailto:hyoung@skku.edu)  
Personal homepage: <http://seclab.skku.edu/people/hyounghick-kim/>

- **Jaehoon (Paul) Jeong**

Assistance 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                      Email: [pauljeong@skku.edu](mailto:pauljeong@skku.edu)  
Personal homepage: <http://iotlab.skku.edu/people-jaehoon-jeong.php>