

Contact Information:

Address: Office #16, 4th Floor, Farmanieh Building, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran, P.O. Box 19395-5531.

Email: hodajannati@ipm.ir

Tell: +98-21-24509416



Employment:

- **Postdoctoral Researcher** Oct.2014-date
Institute for Research in Fundamental Sciences (IPM),
School of Computer Science, Tehran, Iran

Education:

- **Iran University of Science & Technology (IUST)** **Tehran, Iran**
PhD. in Electrical Engineering, Communication Systems Sept.2009-Sept.2014
GPA: 19.06/20
Thesis: Analysis and Design of Distance Bounding Protocols over FRID Noisy Channel
Grade: A
Supervisor: Dr. Abolfazl Falahati
- **Sharif University of Technology (SUT)** **Tehran, Iran**
M.Sc. in Electrical Engineering, Cryptography Communication Sept.2006- Sept. 2008
GPA: 17.51/20
Thesis: Improvement and Analysis of Anonymity Methods in Cryptographic Protocols
Grade: 19.9/20
Supervisor: Dr. Mahmoud Salmasizadeh
- **Technical College of Dr. Shariati (TCS)** **Tehran, Iran**
B.Sc. in Electrical Engineering, Electronics Sept. 2002- Sept. 2006
GPA: 17.29/20
Thesis: Analysis and Simulation of Cross Field Antenna (CFA)
Grade: 19.6/20.
Supervisor: Dr. Vahhab Makki

Research Interest:

- Security issues in RFID, WSN and Cognitive Radio Networks
- Security issues in cloud computing
- Secure Localization and Location Privacy
- Distance Bounding Protocol

Publications:

Journal Papers

1. **Hoda Jannati**, Ebrahim Ardeshir-Larijani and Behnam Bahrak, "Privacy in Cross-User Data Deduplication", *Mobile Networks and Applications*, DOI:s11036-018-1100-5, 2018.
2. **Hoda Jannati** and Behnam Bahrak, "An Improved Authentication Protocol for Distributed Mobile Cloud Computing Services", *International Journal of Critical Infrastructure Protection*, vol. 19, pp. 59-67, 2017.
3. **Hoda Jannati** and Behnam Bahrak, "An Oblivious Transfer Protocol based on Elgamal Encryption for Preserving Location Privacy", *Wireless Personal Communications*, vol. 97(2), pp.3113-3123, 2017.
4. Zeinab Salami, Mahmoud Ahmadian-Attari, **Hoda Jannati** and Mohammad Reza Aref, "A Location Privacy-Preserving Method for Spectrum Sharing in Database-Driven Cognitive Radio Networks", *Wireless Personal Communications*, vol. 95(4), pp.3687-3711, 2017.
5. **Hoda Jannati** and Ebrahim Ardeshir-Larijani, "Detecting Relay Attacks on RFID Communication Systems Using Quantum Bits", *Quantum Information Processing*, vol. 15(11), pp. 4759-4771, 2016.
6. **Hoda Jannati** and Behnam Bahrak, "Security Analysis of an RFID Tag Search Protocol", *Information Processing Letters*, vol. 117(10), pp. 618-622, 2016.
7. **Hoda Jannati**, "Analysis of Relay, Terrorist Fraud and Distance Fraud Attacks on RFID Systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 51-61, 2015.
8. **Hoda Jannati** and Abolfazl Falahati, "An RFID Search Protocol Secured against Relay Attack Based on Distance Bounding Approach," *Wireless Personal Communications*, vol. 85(3), pp. 711-726, 2015.
9. **Hoda Jannati** and Abolfazl Falahati, "Analysis of False-Reject Probability in Distance Bounding Protocols with Mixed Challenges over RFID Noisy Communication Channel," *Information Processing Letters*, vol. 115, pp. 623-629, 2015.
10. **Hoda Jannati** and Abolfazl Falahati, "Achieving an Appropriate Security Level for Distance Bounding Protocols over a Noisy Channel," *Telecommunication Systems*, vol. 58(3), pp. 219-23, 2015.
11. **Hoda Jannati** and Abolfazl Falahati, "An Efficient Mutual Distance Bounding Protocol over a Noisy Channel," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 20(1), pp. 1-16, 2015.

12. **Hoda Jannati** and Abolfazl Falahati, "Mutual Distance Bounding Protocol with its Implementability over a Noisy Channel and its Utilization for Key Agreement in Peer-to-Peer Wireless Networks," *Wireless Personal Communications*, vol. 77(1), pp. 127-149, 2014.
13. Abolfazl Falahati and **Hoda Jannati**, "Distance Bounding-based RFID Binding Proof Protocol to Protect Inpatient Medication Safety against Relay Attack," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 22(2), pp. 71-83, 2016.
14. Abolfazl Falahati and **Hoda Jannati**, "All-or-Nothing Approach to Protect a Distance Bounding Protocol against Terrorist Fraud Attack for Low Cost Devices," *Electronic Commerce Research*, vol. 15, pp. 75-95, 2015.
15. **Hoda Jannati**, Mahmoud Salmasizadeh, Javad Mohajeri and Amir Moradi, "Proxy Zero-Knowledge Proof and Utilization in Anonymous Credential Systems," *Security and Communication Networks*, vol. 6, pp. 161-172, 2013.
16. **Hoda Jannati** and Abolfazl Falahati, "Security Enhanced User Authentication Scheme for Wireless Sensor Network," *International Journal of Electronic Security and Digital Forensic*, vol. 4(4), pp.215-228, 2012.
17. **Hoda Jannati** and Abolfazl Falahati, "Cryptanalysis and Enhancement of Two Low Cost RFID Authentication Protocols," *International Journal of UbiComp*, vol. 3(1), pp. 1-, 2012.

Conference Papers

18. **Hoda Jannati**, Nasour Bagheri and Masoumeh Safkhani, "Analysis of a Distance Bounding Protocol for Verifying the Proximity of Two-Hop Neighbors," *14th International ISC Conference on Information Security and Cryptology (ISCISC'17)*, Shiraz, Iran, IEEE, 2017.
19. Masoumeh Safkhani, **Hoda Jannati** and Nasour Bagheri, "Security Analysis of Niu et al. Authentication and Ownership Management Protocol," *12th Workshop on RFID and IoT Security (RFIDSec'16)*, pp.3-16, vol. 10155 of LNCS, Hong Kong, Springer-Verlag, 2017.
20. **Hoda Jannati** and Abolfazl Falahati, "Analysis of Unilateral Distance Bounding Protocols with Mixed Predefined and Bidirectional Challenges over a Noisy Communication Channel," *22nd Iranian Conference on Electrical Engineering (ICEE'14)*, Tehran, Iran, IEEE, 2014.
21. **Hoda Jannati** and Abolfazl Falahati, "Mutual Implementation of Predefined and Random Challenges over RFID Distance Bounding Protocol," *9th International Conference on Information Security and Cryptology (ISCISC'12)*, pp. 43-47, Tabriz, Iran, IEEE, 2012.

22. Abolfazl Falahati and **Hoda Jannati**, "Application of Distance Bounding Protocols with Random Challenges over RFID Noisy Communication Systems," *IET Conference on Wireless Sensor Systems (WSS'12)*, pp.1-5, 2012.
23. **Hoda Jannati** and Abolfazl Falahati, "Cryptanalysis and Enhancement of a Secure Group Ownership Transfer Protocol for RFID Tags," *International Conference on Global Security, Safety and Sustainability (ICGS3'2011)*, vol 99 of LNICS, pp. 186-193, Thessaloniki, Greece, Springer-Verlag, 2011.
24. **Hoda Jannati** and Abolfazl Falahati, "Proxy Signature Based on Coding Theory," *International Conference on Global Security, Safety and Sustainability (ICGS3'2011)*, vol 92 of CCIS, Braga, Portuguese, pp. 282-290, Springer-Verlag, 2010.
25. **Hoda Jannati**, Mahmoud Salmasizadeh and Javad Mohajeri, "New Proxy Signature and Proxy Blind Signature Based on Okamoto Signature", *2008 International Conference on Security and Management (SAM'08)*, pp. 238-242, Las Vegas, USA, 2008.
26. **Hoda Jannati**, Mahmoud Salmasizadeh and Javad Mohajeri, "Transferable Proxy Signature", *International Conference on Information Security and Cryptology (ISCISC'2008)*, Malek Ashtar University of Technology, Tehran, Iran (In Persian), 2008.

Selected Courses:

- Cryptography Mathematics
- Cryptology and Cryptography
- Advanced Cryptography
- Communications Security
- Network Security
- Neural Network
- Industrial Electronic
- Project Manager
- VLSI
- Wireless Communication
- Advanced Wireless Communication
- Stochastic Processes
- Advanced Communication
- Spread Spectrum Communications
- Information Theory
- Coding Theory
- Digital Signal Processing

Computer Skills:

- Mathematical package
 - ✓ MATLAB and Simulink, Galois, Maple
- Programming languages
 - ✓ C/C++, Visual C, Java, Assembly 8051, FPGA, VHDL, MuxPlus2
- Electronics Software
 - ✓ Orcad, Protel, PSpice, Hspice
- Applications
 - ✓ Microsoft Office, LaTeX, MS Project, SPSS, Photoshop, Front page

Member:

- Executive council of Iranian Society of Cryptography Sept.2017 –Sept. 2018
- Full member of Iranian Society of Cryptography Sept.2009 – date
- Member of society of graduate student of Sharif University of Technology Sept.2008-date
- Head of Iranian Society of Cryptography Student Branch in IUST Sept. 2010 – Sept. 2012
- Student member of Iranian Society of Cryptography Sept.2006 - Sept. 2009
- Student member of IEEE communication society Sept. 2009 - Sept. 2014

Teaching Assistant:

- Coding Theory, IUST Fall 2011, 2012 and 2013
- Cryptology and Cryptography, IUST Fall 2011, 2012 and 2013
- Advanced Wireless Communication, IUST Spring 2012 and 2013
- Communications Security, IUST Fall 2012 and 2013
- Telecommunication Transmission Systems, IUST Spring 2011
- Electronic I, TCS Fall 2005
- Electricity Circuits, TCS Fall 2005

Trainings:

- Lattice-based Cryptography Workshop May 2014
Sharif University of Technology, Tehran, Iran
- Ad-hoc and Sensor Networks Security Workshop April 2011
K. N Toosi University, Tehran, Iran
- RFID Workshop March 2010
LS (Imen Tablo), Grand Hotel, Tehran, Iran
- Integer Factorization Workshop May 2009
Sharif University of Technology, Tehran, Iran
- GSM Workshop May 2008
Sharif University of Technology, Tehran, Iran

Presentation:

- Secure Data Deduplication Methods in Cloud Storage Systems November 2016
Cloud Computing Workshop, Sharif University of Technology
- How to Protect Distance Bounding Protocols against Terrorist Fraud Attack Sept 2016
13th International ISC Conference on Information Security and Cryptology, Shahid Beheshti University of Tehran
- All-or-Nothing Approach to Protect a Distance Bounding Protocol against Terrorist Fraud Attack for Low-Cost Devices March 2015
4th Workshop on Computer Science, IPM
- Bluetooth Security May 2008
GSM workshop, Sharif University of Technology