



Alireza Shafieinejad
Assistant Professor

Tarbiat Modares University,
School of Electrical and Computer Engineering ,
P. O. Box 14115-194, Tehran, IRAN
Office Phone/Fax: +98 21 8288-3247
Email: shafieinejad@modares.ac.ir
Web page: www.modares.ac.ir/~shafieinejad

Education:

- *Ph.D. in Electrical Eng.,* ECE Dep. at IUT, 2006-2012,
 - Under supervision of Dr. Faramarz Hendessi, **GPA:17.3**, Grade **A** for Thesis
- *M.Sc., in Computer Eng.,* ECE Dep. at IUT, 1999-2002,
 - Under supervision of Dr. Faramarz Hendessi, **GPA:15.7**
- *B.Sc. in Computer Eng.,* CE Departement at Sharif University of Technology, 1995-1999
 - **GPA:15.8**

Research Interests:

- Wireless Network Coding
- Cross-Layer Optimization
- Block cipher Design and Analysis
- Network Security Procotols

Publications:

1. Theses:

- [1] **Shafieinejad, A.,** *Network Coding for Multiple Unicast Sessions in Multi-Channel/Interface Wireless Networks (in Persian)*, Ph.D Dissertation, Isfahan University of Technology, Feb 2012
- [2] **Shafieinejad, A.,** *On the Security and performance of the FDE block ciphe (in Persian)* , M.sc Thesis, Isfahan University of Technology, April 2002
- [3] **Shafieinejad, A.,** *Design and Implementation a keyboard for WISE Terminal (in Persian)*, B.sc Thesis, Shafrif University of Technology, June 1999

2. Journal papers:

- [1] **A. Shafieinejad** and F. Hendessi, “Analysis of Inter-flow Network Coding in Lossy Wireless Networks”, *The Modares Journal of Electrical Engineering*, 16(2), pp.62-71 (2016)
- [2] **A. Shafieinejad**, N. Motamedi, , F. Hendessi and M. Mahdavi, "INCP: Practical Wireless Network Coding for Multiple Unicast Sessions", *Springer Wireless Personal Communications*, 91(2), pp.623-651 (2016)
- [3] **A. Shafieinejad**, F. Hendessi and F.Fekri, “Network Coding for multiple unicast sessions in wireless networks”, *Springer Wireless Networks*, Vo. 19, No. 5, pp. 891-911 (2013)
- [4] **A. Shafieinejad**, F. Hendessi and F.Fekri, “Star Structure etwork Coding for multiple unicast sessions in wireless mesh networks”, *Springer Wireless personal communications*, 72(4), 2185-2214
- [5] **A. Shafieinejad** , F. Hendessi and T. A. Gulliver, “*A Structure for Fast Data Encryption*”, *International Journal of Contemp. Math. Sciences*, Vol. 2, 2007, no. 29, 1401 – 1424
- [6] **A. Shafieinejad**, F. Hendessi and T. A. Gulliver, “*On the Security and performance of the FDE block cipher*”, *Contemporary Engineering Sciences*, July 2009, no. 5, 209-238

3. Conference papers:

- [1] M. Fouladian, F. Hendessi, **A. Shafieinejad**, “A New Vertical Handoff Method for 3G/WLAN Networks”, *Proceeding of ICACC 2009, International Conference on Advanced Computer Control Singapore January 22-24, 2009, Singapore Institute of Electronics*
- [2] M.Fouladian, F. Hendessi, **A. Shafieinejad**, “A New Method for Vertical Handoff between WLANs and UMTS in Boundary Conditions ”, *Proceeding of ICCET 2009 , International Conference on Computer Engineering and Technology, Singapore Institute of Electronics*
- [3] **Shafieinejad A**, Hendessi F, N.Azmi, “Security of FDE against Differential and Linearattacks”, *ISCC 2007, Oct 2007*
- [4] **Shafieinejad A**, *Hendessi F*, "Fast C-Implementation of FDE in Software", *ISCC'2003 (The 2th Iranian Society of Cryptology Conference on Cryptology, Comunicatons & Computer Security)*, Oct 2003, pp 11-25

Teaching Experiences:

Tarbiat-Modares University (Graduate):

- Applied Cryptography, 2015-Now (Fall Semester)
- Secure Software Development, 2015-Now (Spring Semester)
- Synthesis of Digital Systems, Spring 2017
- Advanced Computer Architecture, Fall 2016

At Isfahan University of Technology (Under-graduate):

- Computer Networks, Spring 2012
- Data Structure, Fall 2009
- Network Programming, Fall 2008
- Programming in C++, Fall 2008

Awards and Honors:

- Winner of Bronz medal for Iranian Mathematical Olympia
- 159th Rank for global university exam in Iran (Konkur)
- A member of National Institute of Talented Student

Referee:

- **IEEE-TMC:**
 - IEEE Transaction on Mobile Computing
- **ICCK2013:**
 - The 3rd International eConference on Computer and Knowledge Engineering
- **ISSC-2007:**
 - The 5th Iranian Society of Cryptology Conference on Cryptology, Communications & Computer Security

Skills (related to my research interests):

- **Expert in ns-3:** Expert in design, redesign and implementation of network
- **Programming:** expert in C, C++, Python and bash programming
- **Optimization:** expert in AMPL and CPLEX (tools for LP and Convex Optimization)

Work Experiences:

- **Design and developing *Dena* system:**
 - A net-to-net VPN system for both Layer 2 and 3 of protocol stack.
- ***Shams* project : Developing a cryptographic hardware accelerator:**

- For using in KAME IPsec, a version of IPsec that implemented in Linux kernel, to accelerate the process of ESP encryption/decryption.

CoAuthor References:

- *Faramarz Hendessi*,
 - Associate Professor at ECE Department of *Isfahan University of Technology*, Isfahan, Iran
 - My supervisor for both Ph.D and MSc researches.
 - Email : hendessi@cc.iut.ac.ir
- *Faramarz Fekri*,
 - Professor at ECE Department of *Georgia Institute of Technology*, Atlanta, USA
 - My co-supervisor for Ph.D researches
 - Email : faramarz.fekri@gatech.edu
- *Aaron Gulliver*,
 - Professor at ECE Department of *University of Victoria*, British Columbia, Canada
 - My co-supervisor for MSc researches
 - Email : agullive@ece.uvic.ca