Morteza Nikooghadam (Nikoughadam)

Department of Computer Engineering and Information Technology, Imam Reza International University, Mashhad, Iran
Email: m.nikooghadam@imamreza.ac.ir, morteza.nikooghadam@gmail.com
Google Scholar Page, Academic web page, ORCiD
Scopus h-index: 17
WOS h-index: 18

RESEARCH INTERESTS

- Smart Grid Security
- Security Protocols
- Hardware Security
- Galois Field Arithmetic
- Reconfigurable Architectures
- Cryptography

EDUCATIONS

- PhD in Computer Engineering – computer architecture at Shahid Beheshti University, Tehran, Iran — 2008 - 2012
  Thesis: efficient blind signature scheme based on Elliptic Curve Cryptography

- MSc in Computer Engineering – computer architecture at Shahid Beheshti University, Tehran, Iran — 2006 - 2008
  Thesis: efficient implementation of computational components in Elliptic Curve Cryptography on FPGAs

- BSc in Computer Engineering – Hardware at Sadjad University of Technology, Mashhad, Iran — 2002-2006
  Thesis: simulation of a digital signal detector and synchronization of clock using DPLL on FPGA

RESEARCH EXPERIENCES

Journal publications

1. Abbasinezhad-Mood, Dariush, Seyyed Majid Mazinani, Morteza Nikooghadam, and Arezou Ostad Sharif. "Efficient provably-secure dynamic id-based authenticated key agreement scheme with enhanced security provision." *IEEE Transactions on Dependable and Secure Computing* (2020).

2. Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, Sayyed Majid Mazinani, and Morteza Nikooghadam. "Provably Secure Escrow-Less Chebyshev Chaotic Map-Based Key Agreement Protocol for Vehicle to Grid Connections With Privacy Protection." *IEEE Transactions on Industrial Informatics* 16, no. 12 (2020): 7287-7294.

3. Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, Morteza Nikooghadam, and Sayyed Majid Mazinani. "Novel certificateless Chebyshev chaotic map-based key agreement protocol for advanced metering infrastructure." *The Journal of Supercomputing* (2021): 1-29.

4. Eftekhari, Seyed Abdolreza, Morteza Nikooghadam, and Masoud Rafighi. "Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications." *Vehicular Communications* 28 (2021): 100306.

5. Eftekhari, Seyed Abdolreza, Morteza Nikooghadam, and Masoud Rafighi. "Robust session key generation protocol for social internet of vehicles with enhanced security provision." *The Journal of Supercomputing* 77, no. 3 (2021): 2511-2544.
6. Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, and Morteza Nikooghadam. "Efficient provably-secure privacy-preserving signature-based key establishment protocol." *Ad Hoc Networks* 100 (2020): 102062.

7. Abbasinezhad-Mood, Dariush, Morteza Nikooghadam, Sayyed Majid Mazinani, Abolfazl Babamohammadi, and Arezou Ostad-Sharif. "More efficient key establishment protocol for smart grid communications: design and experimental evaluation on ARM-based hardware." *Ad Hoc Networks* 89 (2019): 119-131.

8. Tajmohammadi, Mojtaba, Sayyed Majid Mazinani, Morteza Nikooghadam, and Zahraa Al-Hamdawee. "LSPP: Lightweight and Secure Payment Protocol for Dynamic Wireless Charging of Electric Vehicles in Vehicular Cloud." *IEEE Access* 7 (2019): 148424-148438.

9. Nikooghadam, Morteza, and Ali Zakerolhosseini. "Utilization of pipeline technique in AOP based multipliers with parallel inputs." *Journal of Signal Processing Systems* 72, no. 1 (2013): 57-62.

10. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Efficient design and hardware implementation of a secure communication scheme for smart grid." *International Journal of Communication Systems* 31, no. 10 (2018): e3575.

11. Raei, Hassan, Ensieh Ilkhani, and Morteza Nikooghadam. "SeCARA: A security and cost-aware resource allocation method for mobile cloudlet systems." *Ad Hoc Networks* 86 (2019): 103-118.

12. Ostad-Sharif, Arezou, Abolfazl Babamohammadi, Dariush Abbasinezhad-Mood, and Morteza Nikooghadam. "Efficient privacy-preserving authentication scheme for roaming consumer in global mobility networks." *International Journal of Communication Systems* 32, no. 5 (2019): e3904.

13. Ravanbakhsh, Niloofar, Mohadeseh Mohammadi, and Morteza Nikooghadam. "Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme." *Multimedia Tools and Applications* 78, no. 9 (2019): 11129-11153.

14. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of NanoPi fire." *IEEE Transactions on Reliability* 67, no. 3 (2018): 1328-1339.

15. Moghadam, Mostafa Farhadi, Morteza Nikooghadam, Amir Hossein Mohajerzadeh, and Behzad Movali. "A lightweight key management protocol for secure communication in smart grids." *Electric Power Systems Research* 178 (2020): 106024.

16. Arshad, Hamed, Morteza Nikooghadam, Sara Avezverdi, and Mahboubeh Nazari. "Design and FPGA implementation of an efficient security mechanism for mobile pay-TV systems." *International Journal of Communication Systems* 30, no. 15 (2017): e3305.

17. Ostad-Sharif, Arezou, Dariush Abbasinezhad-Mood, and Morteza Nikooghadam. "An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC." *International Journal of Communication Systems* 32, no. 5 (2019): e3913.

18. Ostad-Sharif, Arezou, Dariush Abbasinezhad-Mood, and Morteza Nikooghadam. "Efficient utilization of elliptic curve cryptography in design of a three-factor authentication protocol for satellite communications." *Computer Communications* 147 (2019): 85-97.

19. Zakerolhosseini, Ali, and Morteza Nikooghadam. "Secure transmission of mobile agent in dynamic distributed environments." *Wireless Personal Communications* 70, no. 2 (2013): 641-656.

20. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Design of an enhanced message authentication scheme for smart grid and its performance analysis on an ARM Cortex-M3 microcontroller." *Journal of information security and applications* 40 (2018): 9-19.

21. Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, Morteza Nikooghadam, and Sayyed Majid Mazinani. "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid." *IEEE Transactions on Industrial Informatics* 16, no. 3 (2019): 1495-1502.

22. Ostad-Sharif, Arezou, Morteza Nikooghadam, and Dariush Abbasinezhad-Mood. "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks." *International Journal of Communication Systems* 32, no. 12 (2019): e3974.

23. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Design and extensive hardware performance analysis of an efficient pairwise key generation scheme for smart grid." *International Journal of Communication Systems* 31, no. 5 (2018): e3507.

24. Nikooghadam, Morteza, and Ali Zakerolhosseini. "An Efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem." *ISeCure* 1, no. 2 (2009).

25. Zakerolhosseini, Ali, and Morteza Nikooghadam. "Low-power and high-speed design of a versatile bit-serial multiplier in finite fields GF (2m)." *Integration, the VLSI journal* 46, no. 2 (2013): 211-217.

26. Abbasinezhad-Mood, Dariush, Arezou Ostad-Sharif, and Morteza Nikooghadam. "Novel anonymous key establishment protocol for isolated smart meters." *IEEE Transactions on Industrial Electronics* 67, no. 4 (2019): 2844-2851.

27. Arshad, Hamed, and Morteza Nikooghadam. "Security analysis and improvement of two authentication and key agreement schemes for session initiation protocol." *The Journal of Supercomputing* 71, no. 8 (2015): 3163-3180.

28. Ostad-Sharif, Arezou, Dariush Abbasinezhad-Mood, and Morteza Nikooghadam. "A robust and efficient ECC-based mutual authentication and session key generation scheme for healthcare applications." *Journal of medical systems* 43, no. 1 (2019): 1-22.

29. Nikooghadam, Morteza, and Ali Zakerolhosseini. "Secure communication of medical information using mobile agents." *Journal of medical systems* 36, no. 6 (2012): 3839-3850.

30. Ostad-Sharif, Arezou, Hamed Arshad, Morteza Nikooghadam, and Dariush Abbasinezhad-Mood. "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme." *Future Generation Computer Systems* 100 (2019): 882-892.

31. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "An ultra-lightweight and secure scheme for communications of smart meters and neighborhood gateways by utilization of an ARM Cortex-M microcontroller." *IEEE Transactions on Smart Grid* 9, no. 6 (2017): 6194-6205.

32. Nikooghadam, Morteza, Ali Zakerolhosseini, and Mohsen Ebrahimi Moghaddam. "Efficient utilization of elliptic curve cryptosystem for hierarchical access control." *Journal of Systems and Software* 83, no. 10 (2010): 1917-1929.

33. Nikooghadam, Morteza, Reza Jahantigh, and Hamed Arshad. "A lightweight authentication and key agreement protocol preserving user anonymity." *Multimedia Tools and Applications* 76, no. 11 (2017): 13401-13423.

34. Mir, Omid, and Morteza Nikooghadam. "A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services." *Wireless Personal Communications* 83, no. 4 (2015): 2439-2461.

35. Arshad, Hamed, Vahid Teymoori, Morteza Nikooghadam, and Hassan Abbassi. "On the security of a two-factor authentication and key agreement scheme for telecare medicine information systems." *Journal of medical systems* 39, no. 8 (2015): 1-10.

36. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications." *Future Generation Computer Systems* 84 (2018): 47-57.

37. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Efficient anonymous password-authenticated key exchange protocol to read isolated smart meters by utilization of extended Chebyshev chaotic maps." *IEEE Transactions on Industrial Informatics* 14, no. 11 (2018): 4815-4828.

38. Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "An anonymous ECC-based self-certified key distribution scheme for the smart grid." *IEEE Transactions on Industrial Electronics* 65, no. 10 (2018): 7996-8004.

39. Arshad, Hamed, and Morteza Nikooghadam. "An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC." *Multimedia Tools and Applications* 75, no. 1 (2016): 181-197.

40. Arshad, Hamed, and Morteza Nikooghadam. "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems." *Journal of medical systems* 38, no. 12 (2014): 1-12.

Conferences

1. Nikooghadam, Morteza; Safaei, Farshad; Zakerolhosseini, Ali; An efficient key management scheme for mobile agents in distributed networks, 2010 1st International Conference on Parallel Distributed and Grid Computing (PDGC), 32-37, 2010, Solan, India.

2. Nikooghadam, Morteza; Malekian, Ehsan; Zakerolhosseini, Ali; A versatile reconfigurable bit-serial multiplier architecture in finite fields GF (2m), Advances in Computer Science and Engineering, 227-234, 2008, Springer, Berlin, Heidelberg

3. Nikooghadam, Morteza; Malekian, Ehsan; Zakerolhosseini, Ali; An Adaptive Architecture For the Bit-Serial multiplication in the Galois Fields GF(2m), 16th Iranian Conference on Electrical Engineering, 2008, Tehran, Iran.

4. Bigonah, Maryam; Abbasinezhad-Mood, Dariush; Nikooghadam, Morteza; Dynamic prioritization and cell fixation placement algorithm based on simulated annealing, 19th International Symposium on Computer Architecture and Digital Systems (CADS), 2017, Kish Island, Iran.

TEACHING EXPERIENCES

- **Computer Architecture**, BSc Level, Ferdowsi University of Mashhad
- **Computer Architecture**, BSc Level, Sadjad University of Technology
- **Computer Architecture**, BSc Level, Imam Reza International University
- **Logical Circuits**, BSc Level, Imam Reza International University
- **Fundamentals of Computer Security**, MSc Level, Imam Reza International University
- **Security protocols**, MSc Level, Imam Reza International University
- **Applied cryptology**, MSc Level, Imam Reza International University
- **Applied cryptography**, MSc Level, Payame Noor University
- **Advanced computer architecture**, Msc Level, Imam Reza International University
- **Basic Systems Security**, BSc Level, Imam Reza International University
- **Advanced Programming**, BSc Imam Reza International University
- **Computer laboratory,** BSc Level, Shahid Beheshti University of Tehran

- **Fundamentals of computer programming,** BSc Level, Shahid Beheshti University of Tehran

SCIENTIFIC SERVICES

REFEREE

- Information Sciences (Elsevier, ISSN: 0020-0255)
- Integration the VLSI journal (Elsevier, ISSN: 0167-9260)
- IEEE Transaction on Smart Grid (IEEE, ISSN: 1949-3053)
- Security and Communication Networks (Wiley, ISSN: 1939-0122)
- Journal of Medical Systems (Springer, ISSN: 1573-689X)
- International Journal of Communication Systems (Wiley, ISSN: 1099-1131)
- Peer-to-Peer Networking and Applications (Springer, ISSN: 1936-6450)
- Wireless Personal Communications (Springer, ISSN: 1572-834X)
- IEEE Transactions on Information Forensics and Security (IEEE, ISSN: 1556-6013)
- IEEE Transactions on Dependable and Secure Computing (IEEE, ISSN: 1545-5971)
- The Computer Journal (Oxford Journals, ISSN: 1460-2067)
- Journal of Medical and Biological Engineering (Springer, ISSN: 2199-4757)

AWARDS

The top researcher in Khorasan province of Iran (branch of engineering), 2021

The best teacher in the university of Imamreza, Mashhad, Iran, 2019

SCIENTIFIC WORKS

Computer group manager, Imamreza University, Mashhad, Iran, 2013-2016

Computer group manager, Imamreza University, Mashhad, Iran, 2018-2021

Supervisor of more than 30 Master of science thesises in Computer Science, Information Security, Computer Architecture, and Electrical Engineering