In the name of God

CURRICULUM VITAE

October, 2019

Nasour Bagheri

	URL: https://sites.google.com/view/nasour-bagheri **Google Scholar:** https://scholar.google.com/citations?hl=en&user=32llx44AAAAJ&view_op=list_works **DBLP:** https://dblp.uni-trier.de/pers/hd/b/Bagheri:Nasour **Publons:** https://publons.com/researcher/1200842/nasour-bagheri/peer-review/	**School Address:** EE. Dept., Shahid Rajaee Teacher Training University Lavizan, Tehran, Iran Nbagheri@srttu.edu Na.bagheri@gmail.com

EDUCATION

- **Iran University of Science and Technology, Tehran, Iran (2004-2010)**

PhD., Electronic Engineering.

Thesis: "*Structural Designing and Analysis of Cryptographic Hash Functions*"

Supervisor: Dr. Majid Naderi

Advisor: Dr. Babak Sadeghiyan

- **Iran University of Science and Technology, Tehran, Iran (2000-2002)**

MSc., Electronic Engineering.

M.S Thesis: "*Design and implementation of a new block cipher*",

Supervisor: Dr. Majid Naderi

Advisor: Dr. Mohsen Sharifi

- **Mazandaran University, Babool, Iran (1996-2000)**

B.Sc., Electronic Engineering.

Senior Project: "*Design a microcontroller based PLC system* ",

Supervisor: Dr Mohsen Soryani

Research Interests

➢ Cryptography (symmetric crypto primitive)

○ Block cipher

- Hash function cryptanalysis
- Stream cipher
- IoT security

- Digital systems
  - Side channels analysis
  - Embedded systems
- Computer security

Publication

1. Journal Publications

1. Hosein Hadipour, Sadegh Sadeghi, Majid M. Niknam, Ling Song, Nasour Bagheri: Comprehensive security analysis of CRAFT, to appear at IACR Trans. Symmetric Cryptology (2020).
2. Mohsen Jahanbani, Zeinolabedin Norouzi, Nasour Bagheri: DPA Protected Implementation of OCB and COLM Authenticated Ciphers. IEEE Access 7: 139815-139826 (2019)
3. Mohsen Jahanbani, Zeinolabedin Norouzi, Nasour Bagheri: Lightweight Implementation of SILC, CLOC, AES-JAMBU and COLM Authenticated Ciphers M Jahanbani, N Bagheri, Z Norozi, Microprocessors and Microsystems, (2019)
4. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: Practical fault resilient hardware implementations of AES. IET Circuits, Devices & Systems 13(5): 596-606 (2019)
5. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: High throughput fault-resilient AES architecture. IET Computers & Digital Techniques 13(4): 312-323 (2019)
6. Akbar Mahmoodi Rishakani, Y. Fekri Dabanloo, Seyed Mojtaba Dehnavi, M. R. Mirzaee Shamsabad, Nasour Bagheri: A Note on the Construction of Lightweight Cyclic MDS Matrices. I. J. Network Security 21(2): 269-274 (2019)
7. Sadegh Sadeghi, Nasour Bagheri: Security analysis of SIMECK block cipher against related-key impossible differential. Inf. Process. Lett. 147: 14-21 (2019)
8. S.Ehsan Hosiny Nezhad; Masoumeh Safkhani; Nasour Bagheri: Relaxed Differential Fault Analysis of SHA-3, The ISC International Journal of Information Security (ISeCure), Volume 11, Issue 2, Pages 129-143 (2019)
9. Akbar Mahmoodi Rishakani; Mohammad Reza Mirzaee Shamsabad; S. M. Dehnavi; Mohammad Amin Amiri; Hamidreza Maimani; Nasour Bagheri :Lightweight 4x4 MDS Matrices for Hardware-Oriented Cryptographic Primitives, The ISC International Journal of Information Security (ISeCure), Volume 11, Issue 1, Pages 35-46, (2019)
10. Masoumeh Safkhani, Nasour Bagheri, Mahyar Shariat: On the Security of Rotation Operation Based Ultra-Lightweight Authentication Protocols for RFID Systems. Future Internet 10(9): 82 (2018)
11. Nasour Bagheri, Seyed Farhad Aghili, Masoumeh Safkhani: On the security of two ownership transfer protocols and their improvements. Int. Arab J. Inf. Technol. 15(1): 87-93 (2018)
12. Sadegh Sadeghi, Nasour Bagheri: Improved zero-correlation and impossible differential cryptanalysis of reduced-round SIMECK block cipher. IET Information Security 12(4): 314-325 (2018)

13. Ygal Bendavid, Nasour Bagheri, Masoumeh Safkhani, Samad Rostampour: IoT Device Security: Challenging "A Lightweight RFID Mutual Authentication Protocol Based on Physical Unclonable Function". Sensors 18(12): 4444 (2018)
14. Mojtaba Eslamnezhad Namin, Mehdi Hosseinzadeh, Nasour Bagheri, Ahmad Khademzadeh: A secure search protocol for lightweight and low-cost RFID systems. Telecommunication Systems 67(4): 539-552 (2018)
15. Samad Rostampour, Nasour Bagheri, Mehdi Hosseinzadeh, Ahmad Khademzadeh: A Scalable and Lightweight Grouping Proof Protocol for Internet of Things Applications. The Journal of Supercomputing 74(1): 71-86 (2018)
16. Nasour Bagheri, Masoumeh Safkhani, Mojtaba Eslamnezhad Namin, Samad Rostampour: An improved low-cost yoking proof protocol based on Kazahaya's flaws. The Journal of Supercomputing 74(5): 1934-1948 (2018)
17. Sadegh Sadeghi, Tahereh Mohammadi, Nasour Bagheri: Cryptanalysis of Reduced round SKINNY Block Cipher. IACR Trans. Symmetric Cryptol. 2018(3): 124-162 (2018)
18. Nasour Bagheri, Parvin Alenaby, Masoumeh Safkhani: A new anti-collision protocol based on information of collided tags in RFID systems. Int. J. Communication Systems 30(3) (2017)
19. Masoumeh Safkhani, Nasour Bagheri, Mehdi Hosseinzadeh, Mojtaba Eslamnezhad Namin, Samad Rostampour: On the security of an RFID-based parking lot management system. Int. J. Communication Systems 30(15) (2017)
20. Sadegh Sadeghi, Nasour Bagheri, Mohamed Ahmed Abdelraheem: Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems - Embedded Hardware Design 52: 34-48 (2017)
21. Masoumeh Safkhani, Nasour Bagheri: Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. The Journal of Supercomputing 73(8): 3579-3585 (2017)
22. Masoumeh Safkhani, Mehdi Hosseinzadeh, Mojtaba Eslamnezhad Namin, Samad Rostampour, Nasour Bagheri: On the (Im)Possibility of Receiving Security Beyond 2 l Using an l-Bit PRNG. Wireless Personal Communications 92(4): 1591-1597 (2017)
23. Praveen Gauravaram, Nasour Bagheri, Lars R. Knudsen: Building indifferentiable compression functions from the PGV compression functions. Des. Codes Cryptogr. 78(2): 547-581 (2016)
24. Samad Rostampour, Nasour Bagheri, Mehdi Hosseinzadeh, Ahmad Khademzadeh: An authenticated encryption based grouping proof protocol for RFID systems. Security and Communication Networks 9(18): 5581-5590 (2016)
25. Masoumeh Safkhani, Nasour Bagheri,: A note on the security of two improved RFID protocols, The ISC International Journal of Information Security (ISeCure), Volume 8, Issue 2, Pages 155-160, (2016)
26. Samad Rostampour; Nasour Bagheri; Mehdi Hosseinzadeh; Ahmad Khademzadeh: On the Security of Permutation Based Authentication Protocols for Internet of Things Applications: The Case of Huang et al.'s Protocol, Journal of Computing and Security (JCS), Volume 3, Issue 4, Page 201-209, (2016)
27. Zahra Zolfaghari; Hamid Asadollahi; Nasour Bagheri: Multicollision Attack on a recently proposed hash function vMDC-2, Journal of Computing and Security (JCS),Volume 3, Issue 4, Page 211-215, (2016)
28. Javad Alizadeh; Mohammad R. Aref; Nasour Bagheri; Hassan Sadeghi: Cryptanalysis of some first round CAESAR candidates, The ISC International Journal of Information Security (ISeCure), Volume 7, Issue 2, Pages 127-134, (2015)
29. Nasour Bagheri, Fatemeh Baghernejhad, Masoumeh Safkhani: On the Designing of EPC C1 G2 Authentication protocol using AKARI-1 and AKARI-2 PRNGs. ITC 44(1): 41-53 (2015)

30. Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, Nasour Bagheri: Weaknesses of fingerprint-based mutual authentication protocol. Security and Communication Networks 8(12): 2124-2134 (2015)
31. Javad Alizadeh; Mohammad Reza Aref; Nasour Bagheri; Alireza Rahimi:JHAE: A Novel Permutation-Based Authenticated Encryption Mode Based on the Hash Mode JH, Journal of Computing and Security (JCS), Volume 2, Issue 1, Page 3-20, (2015)
32. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi: A note on the security of IS-RFID, an inpatient medication safety. I. J. Medical Informatics 83(1): 82-85 (2014)
33. Masoumeh Safkhani, Nasour Bagheri, Ali Mahani: On the security of RFID anti-counting security protocol (ACSP). J. Computational Applied Mathematics 259: 512-521 (2014)
34. Masoumeh Safkhani, Pedro Peris-Lopez, Julio César Hernández Castro, Nasour Bagheri: Cryptanalysis of the Cho et al. protocol: A hash-based RFID tag mutual authentication protocol. J. Computational Applied Mathematics 259: 571-577 (2014)
35. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi: Cryptanalysis of a new EPC class-1 generation-2 standard compliant RFID protocol. Neural Computing and Applications 24(3-4): 799-805 (2014)
36. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, Juan E. Tapiador: Weaknesses in a new ultralightweight RFID authentication protocol with permutation - RAPP. Security and Communication Networks 7(6): 945-949 (2014)
37. N. Bagheri, J. Alizadeh, M.R. Aref "Artemia: A Family of Provably Secure Authenticated Encryption", The ISC International Journal of Information Security, 2014 6 (2).
38. Pablo Picazo-Sanchez, Nasour Bagheri, Pedro Peris-Lopez, Juan E. Tapiador "Two RFID Standard-based Security Protocols for Healthcare Environments" J. Medical Systems 37(5):1-12, 2013. (JCR)
39. Masoumeh Safkhani, Pedro Peris-Lopez, N. Bagheri, M. Safkhani, P. Peris-Lopez and J. E. Tapiador, "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6", IEEE Communications Letters 17(4): 805-807,2013. (JCR)
40. N Bagheri, R Ebrahimpour, N Ghaedi , Differential fault analysis on PRINTcipher, IET Networks 2 (1): 30-36, 2013.
41. M Safkhani, N Bagheri, M Naderi, Strengthening the Security of EPC C-1 G-2 RFID Standard, Wireless Personal Communications, 72(2): 1295-1308 2013. (JCR)
42. N Bagheri, R Ebrahimpour, N Ghaedi: New Differential Fault Analysis on PRESENT, Accepted to appear at EURASIP Journal on Advances in Signal Processing, 2013. (JCR)
43. P. Peris-Lopez, M. Safkhani, N. Bagheri and Majid Naderi, "RFID in eHealth: How Combat Medications Errors and Strengthen Patient Safety", Journal of Medical and Biological Engineering, 2012. (JCR)
44. Nasour Bagheri, Praveen Gauravaram, Lars R. Knudsen, Erik Zenner "The Suffix-free-Prefix-free Hash Function Construction and its Indifferentiability Security Analysis", Int. J. Inf. Sec. 11(6): 419-434 (2012). (JCR)
45. M. Safkhani, N. Bagheri and M. Naderi, "On the Designing of a Tamper Resistant Prescription RFID Access Control System", Journal of Medical Systems, Special Issue on RFID,Vol. 36, pp. 3995-4004, Dec. 2012. (JCR)
46. N. Bagheri, M. Safkhani, M. Naderi, Y. Luo and Q. Chai, "Forgery Attack is a Piece of Cake on a Class of Mutual Authentication Protocols", IJICT, Vol. 3. No. 4, pp. 33-43, June 2012.
47. Amir Ahangi, Mehdi Karamnejad,Nima Mohammadi, Reza Ebrahimpour, Nasour Bagheri "Multiple classifier system for EEG signal classification with application to brain–computer interfaces", accepted to appear at Neural Comput & Applic, 2012. (JCR)
48. Mehdi Azizi, Nasour Bagheri, Abdolrasol Mirgadri "CRYPTANALYSIS OF PASARGAD, A DISTANCE BOUNDING PROTOCOL BASED ON RFID SYSTEM", International Journal of UbiComp (IJU), Vol.3, No.3 pp. 31-42, 2012.

49. Nasour Bagheri “Security Analysis of Zipper Hash Against Multicollisions Attacks”,Engineering, Technology & Applied Science Research ,Vol. 2 No. 3 pp. 226-231, 2012.
50. Javad Alizadeh, Javad Mohajeri and Nasour Bagheri” Linearization Analysis of Two Tweaked Version of MD4 Hash Function”, Journal of Passive Defense Science and Technology, Vol.2, N0-2, pp. 91-100 (in persian), 2011.
51. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi “CRYPTANALYSIS OF SEAS, AN RFID AUTHENTICATION PROTOCOL”, SAIRAN’s journal (in persian), pp. 77-92, 2011.
52. Mehdi Azizi, Nasour Bagheri “Cryptanalysis of SULMA, an Ultralightweight Mutual Authentication Protocol for Low-Cost RFID Tags”, International Journal of UbiComp (IJU), vol. 2, no. 4, pp. 15-25, 2011.
53. Sadegh Jafari, Jaber Karimpour,nasour bagheri “A new secure and practical electronic voting protocol without revealing voters Identity”, International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 6 June 2011, pp. 1291-1299.
54. N.Bagheri, P.Gauravaram, M.Naderi, and B.Sadeghiyan “EPC: A provably secure permutation based compression function” IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences,Vol.E93-A,No.10,pp. 1833-1836, 2010. (JCR)
55. M.Safkhani, M.Naderi, and N.Bagheri, “Cryptanalysis of AFMAP”, IEICE Electronic Express(ELEX) ,2010. (JCR)
56. N.Bagheri, M.Henricksen, L.R.Knudsen, M.Naderi, and B.Sadeghiyan “Cryptanalysis of an Iterated Halving Based Hash Function: CRUSH” IET Inf. Secur., Volume 3, Issue 4, pp.129–138, 2009. (JCR)
57. N.Bagheri, L.R.Knudsen, M.Naderi, and S.S.Thomsen “Hash functions and information theoretic security” IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences,Vol.E92-A,No.12,pp.3041-3043,Dec. 2009. (JCR)

2.Conferences Publications

1. Navid Vafaei, Nasour Bagheri, Sayandeep Saha, Debdeep Mukhopadhyay: Differential Fault Attack on SKINNY Block Cipher. SPACE 2018: 177-197, LNCS .
2. Hoda Jannati, Nasour Bagheri, Masoumeh Safkhani: Analysis of a Distance Bounding Protocol for Verifying the Proximity of Two-Hop Neighbors. ISCISC 2017: 31-36
3. Nasour Bagheri, Florian Mendel, Yu Sasaki: Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ. ACISP (2) 2016: 301-316, LNCS .
4. Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki: Cryptanalysis of Reduced NORX. FSE 2016: 554-574, LNCS .
5. Masoumeh Safkhani, Hoda Jannati, Nasour Bagheri: Security Analysis of Niu et al. Authentication and Ownership Management Protocol. RFIDSec 2016: 3-16, LNCS .
6. Nasour Bagheri: Linear Cryptanalysis of Reduced-Round SIMECK Variants. INDOCRYPT 2015: 140-152, LNCS .
7. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. AlKhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram: Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48. INDOCRYPT 2015: 153-179, LNCS .
8. Nasour Bagheri, Navid Ghaedi, Somitra Kumar Sanadhya: Differential Fault Analysis of SHA-3. INDOCRYPT 2015: 253-269, LNCS .
9. Javad Alizadeh, Hoda AlKhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, Martin M. Lauridsen, Somitra Kumar Sanadhya: Cryptanalysis of SIMON Variants with Connections. RFIDSec 2014: 90-107Nasour

Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya , The Resistance to Intermittent Position Trace Attacks and Desynchronization Attacks (RIPTA-DA) Protocol Is Not RIPTA-DA, RFIDsec 2013,LNCS .

10. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, “Compact hardware implementation of Keccak Hash Function”, NCNIEE, 2013 (in Persian).
11. M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, J. C. Hernandez-Castro, “ Weaknesses in another Gen2-based RFID authentication protocol”, RFID-TA 2012, pp. 80-84, 2012.
12. M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, “ On the traceability of tags in SUAP RFID authentication protocols”, RFID-TA 2012, pp. 292-296, 2012.
13. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, Ali Mahani “On the Security of RFID AntiCloning Security Protocol(ACSP)”, ICACM’12, 2012.
14. Masoumeh Safkhani, Pedro Peris-Lopez, Julio César Hernández Castro, Nasour Bagheri, Majid Naderi “ Cryptanalysis of Cho et al.'s Protocol, A Hash-Based Mutual Authentication Protocol for RFID Systems ICACM’12, 2012.
15. Masoumeh Safkhani, Pedro Peris-Lopez, Nasour Bagheri, Majid Naderi,Julio Cesar Hernandez-Castro “On the Security of Tan et al. Serverless RFID Authentication and Search Protocols”, RFIDsec, 2012.
16. Julio César Hernández Castro, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri, Majid Naderi “ Another Fallen Hash-Based RFID Authentication Protocol”, WISTP 2012: 29-37.
17. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, “Compact hardware implementation of MIBS block cipher”, IKT, 2012 (in Persian).
18. Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, Majid Naderi, “Security Analysis of LMAP++, an RFID Authentication Protocol”, Internet Technology and Secured Transactions (ICITST), 2011.
19. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi “Cryptanalysis of Chen et al.'s RFID Access Control Protocol”, Internet Technology and Secured Transactions (ICITST), 2011.
20. Masoumeh Safkhani, Pedro Peris-Lopez, Nasour Bagheri, Majid Naderi,Julio Cesar Hernandez-Castro “On the Security of Tan et al. Serverless RFID Authentication and Search Protocols”, RFIDsec, LNCS, 2012.
21. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, Yiyuan Luo, Qi Chai “Tag Impersonation Attack on Two RFID Mutual Authentication Protocols”, ARES 2011, pp.581-584.
22. Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, Majid Naderi, and Hamid Behnam “On the Security of Mutual Authentication Protocols for RFID Systems: The Case of Wei et al.'s Protocol”, DPM/SETOP, LNCS, 2011: 90-103.
23. Praveen Gauravaram, Lars R. Knudsen, Nasour Bagheri, Lei Wei” Improved Security Analysis of Fugue-256 (Poster)”, ACISP 2011, LNCS, 428-432.
24. N.Bagheri, L.R.Knudsen, M.Naderi, and S.S.Thomsen "On the Collision and Preimage Resistance of Certain Two-call Hash Functions" , CANS’10, Kuala Lumpur, Malaysia.
25. N.Bagheri, M.Naderi, B.Sadeghiyan “Multi-collisions in Zipper-Hash Structure” Tenth International Symposium on Communication Theory and Applications (ISCTA) 2009, Ambleside, Lake District, UK.
26. N.Bagheri, M.Naderi, B.Sadeghiyan, M.Safkhani “Cryptanalysis of L-Pipe Hash Structure” 17th ICEE 2009, Tehran, Iran.
27. N.Bagheri, M.Naderi, B.Sadeghiyan “A Model for Designing Compression”17th ICEE 2009, Tehran, Iran (In Pesian).
28. N.Bagheri, M.Naderi, B.Sadeghiyan, M.Safkhani “Cryptanalysis of AHS-AES Hash Structure” 13th CSICC 2008, Kish, Iran,(in Persian).

29. N.Bagheri, M.Naderi, B.Sadeghiyan “Multi-collisions in Ring Hash Structure” SECRYPT 2008.
30. Falahati, Aboifazl; Bagheri, Nasoor; Naderi, Majid; Mohajeri, Javad “A new distinguish attack against ABC stream cipher”, The 9th international conference on Advanced Communication Technology, Korea, 2007.
31. N.Bagheri, M.Naderi, “New enhancement to MDx Hash Function class by linear error correction codes”, ISCISC 2007.
32. N.Bagheri, J.Mohajeri, M.Salmasizadeh, “Differential cryptanalysis of AMIN-1 block cipher”, ISCISC 2007, Tehran, Iran.