به نام خداوند بخشنده مهربان

رزومه علمی

نصور باقری

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

استاد تمام
گروه مهندسی مخابرات
دانشگاه تربیت دبیر شهید رجایی، پژوهشکده اکترونیک دانشگاه صنعتی شریف
Nbagheri@sru.ac.ir
Na.bagheri@gmail.com
۰۹۱۲۶۲۳۱۳۳۲

تحصیلات

• دانشگاه علم و صنعت ایران، تهران، ایران (۱۳۸۳–۱۳۸۹) دکتری مهندسی الکترونیک

عنوان رساله دکتری: "طراحی و تحلیل ساختاری توابع چکیده ساز رمزنگاری"

استاد راهنما: دکتر مجید نادری **مشاور:** دکتر بابک صادقیان

• دانشگاه علم و صنعت ایران، تهران، ایران (۱۳۷۹–۱۳۸۱) کارشناس ارشد مهندسی الکترونیک

عنوان پایان نامه کارشناسی ارشد: "طراحی و پیاده سازی یک رمز بلوکی جدید"

استاد راهنما: دکتر مجید نادری **مشاور:** دکتر محسن شریفی

• دانشگاه مازندران، بابل، ایران (۱۳۷۵–۱۳۷۹) کارشناسی، مهندسی الکترونیک

عنوان پروژه کارشناسی: "طراحی یک سیستم PLC مبتنی بر میکروکنترلر"

استاد راهنما: دکتر محسن سریانی

علایق پژوهشی

- **رمز شناسی**
- **امنیت سخت افزار**
- **امنیت شبکه**
- **علوم شناختی**

سوابق اجرایی

سمت	شروع	خاتمه
مدیر گروه الکترونیک	خرداد ۱۳۹۲	اردیبهشت ۱۳۹۲
مدیر فناوری اطلاعات دانشگاه شهید رجایی	اردیبهشت ۱۳۹۲	اردیبهشت ۱۳۹۶
مدیر گروه مهندسی مخابرات	مرداد ۱۴۰۰	مرداد ۱۴۰۳
رئیس دانشکده مهندسی برق	مرداد ۱۴۰۳	آبا ۱۴۰۴

- **عضو حقیقی ستاد توسعه علوم و فناوری افتا (امنیت سایبری) (از خرداد ۱۴۰۴)**
- **عضو شورای اجرایی انجمن رمز ایران (از مهر ۱۴۰۱)**
- **مسئول دبیرخانه دایمی کنفرانس‌های انجمن رمز ایران (از مهر ۱۳۹۹)**

دستاوردهای آموزشی و پژوهشی ۵ سال اخیر

- **پژوهشگر برتر دانشکده (۱۴۰۳)**
- **عضو هیات علمی برتر ارتباط با صنعت دانشگاه (۱۴۰۲)**
- **دریافت نشان درجه یک پژوهش دانشگاه (۱۴۰۱)**
- **پژوهشگر برتر دانشگاه (۱۳۹۹)**
- **استاد راهنمای همکار رساله برتر به انتخاب انجمن رمز ایران (۱۴۰۳)**
- **استاد راهنمای رساله برتر به انتخاب انجمن رمز ایران (۱۴۰۰)**
- **استاد راهنمای پایان نامه شایسته تقدیر به انتخاب انجمن رمز ایران (۱۴۰۲)**
- **نویسنده همکار مقالات برتر مجلات (۱۳۹۶ ، ۱۴۰۰ و ۱۴۰۳) و کنفرانس بین المللی انجمن رمز ایران (۱۴۰۱)**

پروژه ها و طرحها (به عنوان مجری اصلی)

قابل ارائه برحسب درخواست بعد از استعلام

بروندادهای علمی

مقالات مجلات

مقالات منتشره در انتشارات IACR

1. Hadi Soleimany, Nasour Bagheri, Hosein Hadipour, Prasanna Ravi, Shivam Bhasin, Sara Mansouri: Practical Multiple Persistent Faults Analysis. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(1): 367-390 (2022),**CHES 2022**
2. Hadi Soleimany, Nasour Bagheri, Hosein Hadipour, Prasanna Ravi, Shivam Bhasin, Sara Mansouri: Practical Multiple Persistent Faults Analysis. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022(1): 367-390 (2022), **CHES 2022**
3. Hosein Hadipour, Nasour Bagheri, Ling Song: Improved Rectangle Attacks on SKINNY and CRAFT. IACR Trans. Symmetric Cryptol. 2021(2): 140-198 (2021), **FSE 2021**
4. Hosein Hadipour, Sadegh Sadeghi, Majid M. Niknam, Ling Song, Nasour Bagheri: Comprehensive security analysis of CRAFT. IACR Trans. Symmetric Cryptol. 2019(4): 290317 (2019), **FSE 2020**
5. Sadegh Sadeghi, Tahereh Mohammadi, Nasour Bagheri: Cryptanalysis of Reduced round SKINNY Block Cipher. IACR Trans. Symmetric Cryptol. 2018(3): 124-162 (2018), **FSE 2019**
6. Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki: Cryptanalysis of Reduced NORX. FSE 2016: 554-574 (2015). **FSE 2016**

مقالات مرتبط با امنیت و رمزشناسی

7. Narges Mokhtari, Amirhossein Safari, Sadegh Sadeghi, Nasour Bagheri, Samad Rostampour, Ygal Bendavid: "Practical security analysis and attack strategies on permutation functions used in IoT supply chain systems." Scientific Reports 15, no. 1 (2025): 1-15.
8. Alireza Javadi, Sadegh Sadeghi, Peyman Pahlevani, Nasour Bagheri, Samad Rostampour, Ygal Bendavid: Secure and Efficient Lightweight Authentication Protocol (SELAP) for multi-sector IoT applications. Internet Things 30: 101499 (2025)
9. Narges Mokhtari, Navid Vafaei, Sadegh Sadeghi, Nasour Bagheri: Differential Fault Analysis of the BipBip Block Cipher. ISC Int. J. Inf. Secur. 17(2): 223-232 (2025)
10. Sadegh Sadeghi, Nasour Bagheri: Cryptanalysis of DBST, a lightweight block cipher. Frontiers Comput. Sci. 18(4): 184819 (2024)
11. Sajjad Maleki Lonbar, Akram Beigi, Nasour Bagheri, Pedro Peris-Lopez, Carmen Camara: Deep learning based bio-metric authentication system using a high temporal/frequency resolution transform. Frontiers Digit. Health 6 (2024)
12. Nasour Bagheri, Ygal Bendavid, Masoumeh Safkhani, Samad Rostampour: Smart Grid Security: A PUF-Based Authentication and Key Agreement Protocol. Future Internet 16(1): 9 (2024)
13. Nasser Zarbi, Ali Zaeembashi, Nasour Bagheri, Morteza Adeli: Toward designing a lightweight RFID authentication protocol for constrained environments. IET Commun. 18(14): 846-859 (2024)
14. Morteza Adeli, Nasour Bagheri, Hamid Reza Maimani, Saru Kumari, Joel J. P. C. Rodrigues: A Post-Quantum Compliant Authentication Scheme for IoT Healthcare Systems. IEEE Internet Things J. 11(4): 6111-6118 (2024)
15. Ygal Bendavid, Samad Rostampour, Yacine Berrabah, Nasour Bagheri, Masoumeh Safkhani: The Rise of Passive RFID RTLS Solutions in Industry 5.0. Sensors 24(5): 1711 (2024)

16. Samad Rostampour, Nasour Bagheri, Behnam Ghavami, Ygal Bendavid, Saru Kumari, Honorio Martín, Carmen Camara: Using a privacy-enhanced authentication process to secure IoT-based smart grid infrastructures. J. Supercomput. 80(2): 1668-1693 (2024)
17. Navid Vafaei, Hadi Soleimany, Nasour Bagheri: Exploiting statistical effective fault attack in a blind setting. IET Inf. Secur. 17(4): 639-646 (2023)
18. Morteza Adeli, Nasour Bagheri, Sadegh Sadeghi, Saru Kumari: χperbp: a cloud-based lightweight mutual authentication protocol. Peer Peer Netw. Appl. 16(4): 1785-1802 (2023)
19. Carmen Camara, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri: ECG Identification Based on the Gramian Angular Field and Tested with Individuals in Resting and Activity States. Sensors 23(2): 937 (2023)
20. Carmen Camara, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri: ECGsound for human identification. Biomed. Signal Process. Control. 72(Part): 103335 (2022)
21. Samad Rostampour, Nasour Bagheri, Ygal Bendavid, Masoumeh Safkhani, Saru Kumari, Joel J. P. C. Rodrigues: An Authentication Protocol for Next Generation of Constrained IoT Systems. IEEE Internet Things J. 9(21): 21493-21504 (2022)
22. Navid Vafaei, Maryam Porkar, Hamed Ramzanipour, Nasour Bagheri: Practical Differential Fault Analysis on SKINNY. ISC Int. J. Inf. Secur. 14(3): 9-19 (2022)
23. Hamed Ramzanipour, Navid Vafaei, Nasour Bagheri: Practical Differential Fault Analysis on CRAFT, a Lightweight Block Cipher. ISC Int. J. Inf. Secur. 14(3): 21-31 (2022)
24. Masoumeh Safkhani, Samad Rostampour, Ygal Bendavid, Sadegh Sadeghi, Nasour Bagheri: Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols. J. Inf. Secur. Appl. 67: 103194 (2022)
25. Morteza Adeli, Nasour Bagheri, Honorio Martín, Pedro Peris-Lopez: Challenging the security of "A PUF-based hardware mutual authentication protocol". J. Parallel Distributed Comput. 169: 199-210 (2022)
26. Nasour Bagheri, Saru Kumari, Carmen Camara, Pedro Peris-Lopez: Defending Industry 4.0: An Enhanced Authentication Scheme for IoT Devices. IEEE Syst. J. 16(3): 4501-4512 (2022)
27. Navid Vafaei, Sara Zarei, Nasour Bagheri, Maria Eichlseder, Robert Primas, Hadi Soleimany: Statistical Effective Fault Attacks: The Other Side of the Coin. IEEE Trans. Inf. Forensics Secur. 17: 1855-1867 (2022)
28. Akbar Mahmoodi Rishakani, Seyed Mojtaba Dehnavi, Mohammad Reza Mirzaee Shamsabad, Nasour Bagheri: Cryptographic properties of cyclic binary matrices. Adv. Math. Commun. 15(2): 311-327 (2021)
29. Sadegh Sadeghi, Vincent Rijmen, Nasour Bagheri: Proposing an MILP-based method for the experimental verification of difference-based trails: application to SPECK, SIMECK. Des. Codes Cryptogr. 89(9): 2113-2155 (2021)
30. Morteza Adeli, Nasour Bagheri, Hamid Reza Meimani: On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments. J. Ambient Intell. Humaniz. Comput. 12(2): 3075-3089 (2021)
31. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: Reliable advanced encryption standard hardware implementation: 32- bit and 64-bit data-paths. Microprocess. Microsystems 81: 103740 (2021)
32. Morteza Adeli, Nasour Bagheri: MDSbSP: a search protocol based on MDS codes for RFID-based Internet of vehicle. J. Supercomput. 77(2): 1094-1113 (2021)
33. Masoumeh Safkhani, Carmen Camara, Pedro Peris-Lopez, Nasour Bagheri: RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. Veh. Commun. 28: 100311 (2021)

34. Mehdi Hosseinzadeh, Jan Lansky, Amir Masoud Rahmani, Cuong Trinh, Masoumeh Safkhani, Nasour Bagheri, Bao Huynh: A New Strong Adversary Model for RFID Authentication Protocols. IEEE Access 8: 125029-125045 (2020)
35. Mehdi Hosseinzadeh, Omed Hassan Ahmed, Sarkar Hasan Ahmed, Cuong Trinh, Nasour Bagheri, Saru Kumari, Jan Lansky, Bao Huynh: An Enhanced Authentication Protocol for RFID Systems. IEEE Access 8: 126977-126987 (2020)
36. Cuong Trinh, Bao Huynh, Jan Lansky, Stanislava Mildeová, Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Mehdi Hosseinzadeh: A Novel Lightweight Block Cipher-Based Mutual Authentication Protocol for Constrained Environments. IEEE Access 8: 165536-165550 (2020)
37. Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Hamidreza Tavakoli, Sachin Kumar, Jiahui Chen: RESEAP: An ECC-Based Authentication and Key Agreement Scheme for IoT Applications. IEEE Access 8: 200851-200862 (2020)
38. Masoumeh Safkhani, Samad Rostampour, Ygal Bendavid, Nasour Bagheri: IoT in medical & pharmaceutical: Designing lightweight RFID security protocols for ensuring supply chain integrity. Comput. Networks 181: 107558 (2020)
39. Majid M. Niknam, Sadegh Sadeghi, Mohammad Reza Aref, Nasour Bagheri: Investigation of Some Attacks on GAGE (v1), InGAGE (v1), (v1.03), and CiliPadi (v1) Variants. ISC Int. J. Inf. Secur. 12(1): 13-23 (2020)
40. Mohsen Jahanbani, Nasour Bagheri, Zynolabedin Norouzi: CPA on COLM Authenticated Cipher and the Protection Using Domain-Oriented Masking. ISC Int. J. Inf. Secur. 12(2): 67-80 (2020)
41. Navid Vafaei, Sayandeep Saha, Nasour Bagheri, Debdeep Mukhopadhyay: Fault Attack on SKINNY Cipher. J. Hardw. Syst. Secur. 4(4): 277-296 (2020)
42. Mohsen Jahanbani, Nasour Bagheri, Zeinolabedin Norouzi: Lightweight implementation of SILC, CLOC, AES-JAMBU and COLM authenticated ciphers. Microprocess. Microsystems 72 (2020)
43. Samad Rostampour, Masoumeh Safkhani, Ygal Bendavid, Nasour Bagheri: ECCbAP: A secure ECC-based authentication protocol for IoT edge devices. Pervasive Mob. Comput. 67: 101194 (2020)
44. Mohsen Jahanbani, Zeinolabedin Norouzi, Nasour Bagheri: DPA Protected Implementation of OCB and COLM Authenticated Ciphers. IEEE Access 7: 139815-139826 (2019)
45. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: Practical fault resilient hardware implementations of AES. IET Circuits Devices Syst. 13(5): 596-606 (2019)
46. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: High throughput fault-resilient AES architecture. IET Comput. Digit. Tech. 13(4): 312-323 (2019)
47. Akbar Mahmoodi Rishakani, Yousef Fekri Dabanloo, Seyed Mojtaba Dehnavi, Mohammad Reza Mirzaee Shamsabad, Nasour Bagheri: A Note on the Construction of Lightweight Cyclic MDS Matrices. Int. J. Netw. Secur. 21(2): 269-274 (2019)
48. Sadegh Sadeghi, Nasour Bagheri: Security analysis of SIMECK block cipher against related-key impossible differential. Inf. Process. Lett. 147: 14-21 (2019)
49. Akbar Mahmoodi Rishakani, Mohammad Reza Mirzaee Shamsabad, Seyed Mojtaba Dehnavi, Mohammad Amin Amiri, Hamidreza Maimani, Nasour Bagheri: Lightweight 4x4 MDS Matrices for Hardware-Oriented Cryptographic Primitives. ISC Int. J. Inf. Secur. 11(1): 35-46 (2019)
50. S. Ehsan Hosiny Nezhad, Masoumeh Safkhani, Nasour Bagheri: Relaxed Differential Fault Analysis of SHA-3. ISC Int. J. Inf. Secur. 11(2): 129-143 (2019)

51. 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)
52. 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)
53. Sadegh Sadeghi, Nasour Bagheri: Improved zero-correlation and impossible differential cryptanalysis of reduced-round SIMECK block cipher. IET Inf. Secur. 12(4): 314-325 (2018)
54. 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)
55. Mojtaba Eslamnezhad Namin, Mehdi Hosseinzadeh, Nasour Bagheri, Ahmad Khademzadeh: A secure search protocol for lightweight and low-cost RFID systems. Telecommun. Syst. 67(4): 539-552 (2018)
56. Samad Rostampour, Nasour Bagheri, Mehdi Hosseinzadeh, Ahmad Khademzadeh: A Scalable and Lightweight Grouping Proof Protocol for Internet of Things Applications. J. Supercomput. 74(1): 71-86 (2018)
57. Nasour Bagheri, Masoumeh Safkhani, Mojtaba Eslamnezhad Namin, Samad Rostampour: An improved low-cost yoking proof protocol based on Kazahaya's flaws. J. Supercomput. 74(5): 1934-1948 (2018)
58. Nasour Bagheri, Parvin Alenaby, Masoumeh Safkhani: A new anti-collision protocol based on information of collided tags in RFID systems. Int. J. Commun. Syst. 30(3) (2017)
59. Masoumeh Safkhani, Nasour Bagheri, Mehdi Hosseinzadeh, Mojtaba Eslamnezhad Namin, Samad Rostampour: On the security of an RFID-based parking lot management system. Int. J. Commun. Syst. 30(15) (2017)
60. Sadegh Sadeghi, Nasour Bagheri, Mohamed Ahmed Abdelraheem: Cryptanalysis of reduced QTL block cipher. Microprocess. Microsystems 52: 34-48 (2017)
61. Masoumeh Safkhani, Nasour Bagheri: Passive secret disclosure attack on an ultralightweight authentication protocol for Internet of Things. J. Supercomput. 73(8): 3579-3585 (2017)
62. 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. Wirel. Pers. Commun. 92(4): 1591-1597 (2017)
63. Praveen Gauravaram, Nasour Bagheri, Lars R. Knudsen: Building indifferentiable compression functions from the PGV compression functions. Des. Codes Cryptogr. 78(2): 547-581 (2016)
64. Masoumeh Safkhani, Nasour Bagheri: A note on the security of two improved RFID protocols. ISC Int. J. Inf. Secur. 8(2): 155-160 (2016)
65. Samad Rostampour, Nasour Bagheri, Mehdi Hosseinzadeh, Ahmad Khademzadeh: An authenticated encryption based grouping proof protocol for RFID systems. Secur. Commun. Networks 9(18): 5581-5590 (2016)
66. Javad Alizadeh, Mohammad Reza Aref, Nasour Bagheri, Hassan Sadeghi: Cryptanalysis of some first round CAESAR candidates. ISC Int. J. Inf. Secur. 7(2): 127-134 (2015)
67. Nasour Bagheri, Fatemeh Baghernejhad, Masoumeh Safkhani: On the Designing of EPC C1 G2 Authentication protocol using AKARI-1 and AKARI-2 PRNGs. Inf. Technol. Control. 44(1): 41-53 (2015)
68. Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, Nasour Bagheri: Weaknesses of fingerprint-based mutual authentication protocol. Secur. Commun. Networks 8(12): 2124-2134 (2015)
69. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi: A note on the security of IS-RFID, an inpatient medication safety. Int. J. Medical Informatics 83(1): 82-85 (2014)

70. Javad Alizadeh, Mohammad Reza Aref, Nasour Bagheri: Artemia: a family of provably secure authenticated encryption schemes. ISC Int. J. Inf. Secur. 6(2): 125-139 (2014)
71. Masoumeh Safkhani, Nasour Bagheri, Ali Mahani: On the security of RFID anti-counting security protocol (ACSP). J. Comput. Appl. Math. 259: 512-521 (2014)
72. 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. Comput. Appl. Math. 259: 571-577 (2014)
73. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi: Cryptanalysis of a new EPC class-1 generation-2 standard compliant RFID protocol. Neural Comput. Appl. 24(3-4): 799-805 (2014)
74. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, Juan E. Tapiador: Weaknesses in a new ultralightweight RFID authentication protocol with permutation - RAPP. Secur. Commun. Networks 7(6): 945-949 (2014)
75. Nasour Bagheri, Reza Ebrahimpour, Navid Ghaedi: New differential fault analysis on PRESENT. EURASIP J. Adv. Signal Process. 2013: 145 (2013)
76. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, Juan E. Tapiador: Comments on "Security Improvement of an RFID Security Protocol of ISO/IEC WD 29167-6". IEEE Commun. Lett. 17(4): 805-807 (2013)
77. Nasour Bagheri, Reza Ebrahimpour, Navid Ghaedi: Differential fault analysis on PRINTcipher. IET Networks 2(1) (2013)
78. Pablo Picazo-Sanchez, Nasour Bagheri, Pedro Peris-Lopez, Juan E. Tapiador: Two RFID Standard-based Security Protocols for Healthcare Environments. J. Medical Syst. 37(5): 9962 (2013)
79. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi: Strengthening the Security of EPC C-1 G-2 RFID Standard. Wirel. Pers. Commun. 72(2): 1295-1308 (2013)
80. 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)
81. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi: On the Designing of a Tamper Resistant Prescription RFID Access Control System. J. Medical Syst. 36(6): 3995-4004 (2012)
82. Masoumeh Safkhani, Majid Naderi, Nasour Bagheri: Cryptanalysis of AFMAP. IEICE Electron. Express 7(17): 1240-1245 (2010)
83. Nasour Bagheri, Praveen Gauravaram, Majid Naderi, Babak Sadeghiyan: EPC: A Provably Secure Permutation Based Compression Function. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 93-A(10): 1833-1836 (2010)
84. Nasour Bagheri, Lars R. Knudsen, Majid Naderi, Søren S. Thomsen: Hash Functions and Information Theoretic Security. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 92-A(12): 3401-3403 (2009)
85. Nasour Bagheri, Matt Henricksen, Lars R. Knudsen, Majid Naderi, B. Sadeghyian: Cryptanalysis of an iterated halving-based hash function: CRUSH. IET Inf. Secur. 3(4): 129-138 (2009)

مقالات حوزه علوم شناختی

86. Mohammad Hossein Karimi, Reza Ebrahimpour, Nasour Bagheri: A Recurrent Temporal Model for Semantic Levels Categorization Based on Human Visual System. Comput. Intell.
87. Neurosci. 2021: 8895579:1-8895579:20 (2021)
88. Mohammad Hossein Karimi, Reza Ebrahimpour, Nasour Bagheri: Object Categorization at the Higher Levels Do With More Neurons Than Finer Levels and Takes Faster. IEEE Access 9: 32873-32881 (2021)
89. Alireza Mohammadi Anbaran, Pooya Torkzadeh, Reza Ebrahimpour, Nasour Bagheri: Modification and hardware implementation of cortex-like object recognition model. IET Image Process. 14(14): 3490-3498 (2020)
90. H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour Invariant object recognition is a personalized selection of invariant features in humans, not simply explained by hierarchical feed-forward vision models - Scientific reports, 2017
91. H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour Hard-wired feed-forward visual mechanisms of the brain compensate for affine variations in object recognition - Neuroscience, 2017
92. Amir Ahangi, Mehdi Karamnejad,Nima Mohammadi, Reza Ebrahimpour, Nasour
93. Bagheri "Multiple classifier system for EEG signal classification with application to braincomputer interfaces", accepted to appear at Neural Comput & Applic, 2012. (JCR)
94. H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour , Average activity, but not variability, is the dominant factor in the representation of object categories in the brain - Neuroscience, 2017

مقالات همایش

1. Mahdi Nikooghadam,, Haleh Amintoosi, and Nasour Bagheri: Lightweight Authentication for Remote Healthcare Systems in Cloud-IoT. 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE). **IEEE**, 2020.
2. Navid Vafaei, Nasour Bagheri, Sayandeep Saha, Debdeep Mukhopadhyay: Differential Fault Attack on SKINNY Block Cipher. SPACE 2018: 177-197, **LNCS** .
3. Hoda Jannati, Nasour Bagheri, Masoumeh Safkhani: Analysis of a Distance Bounding Protocol for Verifying the Proximity of Two-Hop Neighbors. ISCISC 2017: 31-36
4. Nasour Bagheri, Florian Mendel, Yu Sasaki: Improved Rebound Attacks on AESQ: Core Permutation of CAESAR Candidate PAEQ. ACISP (2) 2016: 301-316, **LNCS**.
5. Nasour Bagheri, Tao Huang, Keting Jia, Florian Mendel, Yu Sasaki: Cryptanalysis of Reduced NORX. FSE 2016: 554-574, **LNCS**.
6. Masoumeh Safkhani, Hoda Jannati, Nasour Bagheri: Security Analysis of Niu et al. Authentication and Ownership Management Protocol. RFIDSec 2016: 3-16, LNCS.
7. Nasour Bagheri: Linear Cryptanalysis of Reduced-Round SIMECK Variants. INDOCRYPT 2015: 140-152, LNCS.
8. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. AlKhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram: Improved Linear Cryptanalysis of ReducedRound SIMON-32 and SIMON-48. INDOCRYPT 2015: 153-179, LNCS.
9. Nasour Bagheri, Navid Ghaedi, Somitra Kumar Sanadhya: Differential Fault Analysis of SHA-3. INDOCRYPT 2015: 253-269, LNCS.
10. 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: 90-107

11. Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya , The Resistance to Intermittent Position Trace Attacks and Desynchronization Attacks (RIPTADA) Protocol Is Not RIPTA-DA, RFIDsec 2013, LNCS.
12. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, "Compact hardware implementation of Keccak Hash Function", NCNIEE, 2013 (in Persian).
13. 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. 8084, 2012, **IEEE**.
14. 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, **IEEE**.
15. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, Ali Mahani "On the Security of RFID AntiCloning Security Protocol(ACSP)", ICACM'12, 2012, **IEEE**.
16. 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.
17. 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, **LNCS**.
18. Julio César Hernández Castro, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri, Majid Naderi " Another Fallen Hash-Based RFID Authentication Protocol", WISTP 2012: 29-37, **LNCS**.
19. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, "Compact hardware implementation of MIBS block cipher", IKT, 2012 (in Persian).
20. Masoumeh Safkhani, Nasour Bagheri, Somitra Kumar Sanadhya, Majid Naderi, "Security Analysis of LMAP++, an RFID Authentication Protocol", Internet Technology and Secured Transactions (ICITST), 2011, **IEEE**.
21. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi "Cryptanalysis of Chen et al.'s RFID Access Control Protocol", Internet Technology and Secured Transactions (ICITST), 2011, **IEEE**.
22. 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.
23. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, Yiyuan Luo, Qi Chai "Tag Impersonation Attack on Two RFID Mutual Authentication Protocols", ARES 2011, pp.581-584, **IEEE**.
24. 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.
25. Praveen Gauravaram, Lars R. Knudsen, Nasour Bagheri, Lei Wei" Improved Security Analysis of Fugue-256 (Poster)", ACISP 2011, **LNCS**, 428-432.
26. 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,**LNCS**.
27. 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.

28. N.Bagheri, M.Naderi, B.Sadeghiyan, M.Safkhani “Cryptanalysis of L-Pipe Hash Structure” 17th ICEE 2009, Tehran, Iran.
29. N.Bagheri, M.Naderi, B.Sadeghiyan “A Model for Designing Compression”17th ICEE 2009, Tehran, Iran (In Persian).
30. N.Bagheri, M.Naderi, B.Sadeghiyan, M.Safkhani “Cryptanalysis of AHS-AES Hash Structure” 13th CSICC 2008, Kish, Iran,(in Persian).
31. N.Bagheri, M.Naderi, B.Sadeghiyan “Multi-collisions in Ring Hash Structure” SECRYPT 2008.
32. 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.
33. N.Bagheri, M.Naderi, “New enhancement to MDx Hash Function class by linear error correction codes”, ISCISC 2007.
34. N.Bagheri, J.Mohajeri, M.Salmasizadeh, “Differential cryptanalysis of AMIN-1 block cipher”, ISCISC 2007, Tehran, Iran.