به نام خداوند بخشنده مهربان

رزومه علمی

نصور باقری

بهمن ۱۴۰۲

	**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/nasourbagheri/peer-review/	**استاد تمام** **گروه مهندسی مخابرات دانشگاه تربیت دبیر شهید رجایی** Nbagheri@sru.ac.ir Na.bagheri@gmail.com

تحصیلات

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

پایان نامه: 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.

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.

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

استاد راهنما: دکتر محسن سوریانی

علایق پژوهشی

- **رمز شناسی**
- **امنیت سخت افزاری**
- **امنیت کامپیوتر**
- **علوم شناختی**

پروژه ها و طرح‌های برون دانشگاهی اجرا شده (به عنوان مجری اصلی)

طرف قرارداد	عنوان	مبلغ (میلیون ریال)	تاریخ شروع	تاریخ خاتمه
شورای محترم نگهبان	قابل ارائه برحسب درخواست بعد از استعلام	۶۵۰۰	۱۳۹۹	۱۴۰۰
مرکز تحقیقات صدر	قابل ارائه برحسب درخواست بعد از استعلام	۵۰۰	۱۴۰۰	۱۴۰۱
مرکز فاوای وزارت دفاع	قابل ارائه برحسب درخواست بعد از استعلام	۱۸۰۰	۱۴۰۰	۱۴۰۲
مرکز فاوای وزارت دفاع	قابل ارائه برحسب درخواست بعد از استعلام	۲۰۰۰	۱۴۰۰	۱۴۰۲
مرکز ارزیابی سامانه های امنیتی فاوا(مساف) دانشگاه امام حسین	قابل ارائه برحسب درخواست بعد از استعلام	-	-	-
INSF	تحلیل امنیت رمزهای متقارن سبک با تمرکز بر مسابقه استاندارد سازی NIST LWC، با رویکرد توسعه خودکار سازی تحلیل	۲۵۰	۱۳۹۸/۹/۱۶	۱۴۰۱/۳/۱۰
پژوهشکده علوم کامپیوتر IPM	تحلیل امنیتی و طراحی پروتکل‌های احراز اصالت و اشتراک کلید سبک وزن نوین برای اینترنت اشیاء با هدف ارائه مدلهای مهاجم نوین	۱۵۰	۱۴۰۰/۱/۱	۱۴۰۰/۱۲/۲۹
پژوهشکده علوم کامپیوتر IPM	تحلیل امنیت رمزهای متقارن سبک با تمرکز بر کاندیداهای مسابقه استاندارد سازی NIST-LWC	۱۵۰	۱۳۹۹/۱/۱	۱۳۹۹/۱۲/۲۹
پژوهشکده علوم کامپیوتر IPM	توسعه ابزارهای تحلیل خودکار برای تحلیل رمزهای متقارن	۱۵۰	۱۳۹۸/۱/۱	۱۳۹۸/۱۲/۲۹
پژوهشکده علوم کامپیوتر IPM	تحلیل امنیت الگوریتمهای رمز متقارن به کمک روشهای خودکار۲	۱۲۰	۱۳۹۷/۱/۱	۱۳۹۷/۱۲/۲۹
پژوهشکده علوم کامپیوتر IPM	تحلیل امنیت الگوریتم های رمز متقارن به کمک روش های خودکار۱	۱۲۰	۱۳۹۶/۱/۱	۱۳۹۶/۱۲/۲۹
پژوهشکده علوم کامپیوتر IPM	تحلیل و بررسی امنیت رمز متقارن	۱۲۰	۱۳۹۴/۶/۱	۱۳۹۵/۱۲/۲۹

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): 290-317 (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 رمزشناسی

7. Adeli, Morteza, Nasour Bagheri, Hamid Reza Maimani, Saru Kumari, and Joel JPC Rodrigue: A Post-Quantum Compliant Authentication Scheme for IoT Healthcare Systems. IEEE Internet Things J. 11(4): (2024)
8. 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)
9. Navid Vafaei, Hadi Soleimany, Nasour Bagheri: Exploiting statistical effective fault attack in a blind setting. IET Inf. Secur. 17(4): 639-646 (2023)
10. 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)
11. 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)
12. Carmen Camara, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri: ECGsound for human identification. Biomed. Signal Process. Control. 72(Part): 103335 (2022)
13. 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)
14. Navid Vafaei, Maryam Porkar, Hamed Ramzanipour, Nasour Bagheri: Practical Differential Fault Analysis on SKINNY. ISC Int. J. Inf. Secur. 14(3): 9-19 (2022)

15. 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)
16. 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)
17. 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)
18. 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)
19. 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)
20. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: Reliable advanced encryption standard hardware implementation: 32- bit and 64-bit data-paths. Microprocess. Microsystems 81: 103740 (2021)
21. 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)
22. Navid Vafaei, Sayandeep Saha, Nasour Bagheri, Debdeep Mukhopadhyay: Fault Attack on SKINNY Cipher. J. Hardw. Syst. Secur. 4(4): 277-296 (2020)
23. 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) **(Best Paper)**
24. 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)
25. 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)
26. Sadegh Sadeghi, Nasour Bagheri: Security analysis of SIMECK block cipher against related-key impossible differential. Inf. Process. Lett. 147: 14-21 (2019)
27. 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)
28. Praveen Gauravaram, Nasour Bagheri, Lars R. Knudsen: Building indifferentiable compression functions from the PGV compression functions. Des. Codes Cryptogr. 78(2): 547-581 (2016)
29. 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)
30. 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)
31. 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).

32. 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)
33. 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)

مقالات حوزه امنیت

34. Carmen Camara, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri: ECGsound for human identification. Biomed. Signal Process. Control. 72(Part): 103335 (2022)
35. 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)
36. 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)
37. 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)
38. 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)
39. Safkhani, Masoumeh, Samad Rostampour, Ygal Bendavid, Sadegh Sadeghi, and Nasour Bagheri. "Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols." Journal of Information Security and Applications 67 (2022): 103194.
40. Nasour Bagheri, Saru Kumari, Carmen Camara, Pedro Peris-Lopez: "Defending Industry 4.0: An Enhanced Authentication Scheme for IoT Devices." IEEE Systems Journal (2021).
41. Carmen Camara, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri: ECGsound for human identification. Biomed. Signal Process. Control. 72(Part): 103335 (2022)
42. 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)
43. 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)
44. 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)
45. 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)
46. Mohsen Jahanbani, Nasour Bagheri, Zeinolabedin Norouzi: Lightweight implementation of SILC, CLOC, AES-JAMBU and COLM authenticated ciphers. Microprocess. Microsystems 72 (2020)
47. 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)

48. 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)
49. 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)
50. 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)
51. 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)
52. Mohsen Jahanbani, Zeinolabedin Norouzi, Nasour Bagheri: DPA Protected Implementation of OCB and COLM Authenticated Ciphers. IEEE Access 7: 139815139826 (2019)
53. 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)
54. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: Practical fault resilient hardware implementations of AES. IET Circuits, Devices & Systems 13(5): 596-606 (2019)
55. Saeide Sheikhpour, Ali Mahani, Nasour Bagheri: High throughput fault-resilient AES architecture. IET Computers & Digital Techniques 13(4): 312-323 (2019)
56. 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)
57. 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)
58. 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): 8793 (2018)
59. 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)
60. 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)
61. 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)
62. 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)
63. 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)

64. 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)
65. Sadegh Sadeghi, Nasour Bagheri, Mohamed Ahmed Abdelraheem: Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems - Embedded Hardware Design 52: 34-48 (2017)
66. 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)
67. 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)
68. 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)
69. 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)
70. 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)
71. 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)
72. 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)
73. 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)
74. 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)
75. Masoumeh Safkhani, Nasour Bagheri, Ali Mahani: On the security of RFID anti-counting security protocol (ACSP). J. Computational Applied Mathematics 259: 512-521 (2014)
76. 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)
77. 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)
78. 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)
79. 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)

80. 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)
81. N Bagheri, R Ebrahimpour, N Ghaedi , Differential fault analysis on PRINTcipher, IET Networks 2 (1): 30-36, 2013.
82. 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)
83. 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)
84. 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)
85. 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.
86. 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.
87. Nasour Bagheri "Security Analysis of Zipper Hash Against Multicollisions Attacks",Engineering, Technology & Applied Science Research ,Vol. 2 No. 3 pp. 226231, 2012.
88. 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.
89. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi "CRYPTANALYSIS OF SEAS, AN RFID AUTHENTICATION PROTOCOL", SAIRAN's journal (in persian), pp. 77-92, 2011.
90. 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.
91. 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.
92. 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)
93. M.Safkhani, M.Naderi, and N.Bagheri, "Cryptanalysis of AFMAP", IEICE Electronic Express(ELEX) ,2010. (JCR)
94. 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)

مقالات حوزه علوم شناختی

95. Mohammad Hossein Karimi, Reza Ebrahimpour, Nasour Bagheri: A Recurrent Temporal Model for Semantic Levels Categorization Based on Human Visual System. Comput. Intell. Neurosci. 2021: 8895579:1-8895579:20 (2021)
96. 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)
97. 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)
98. Invariant object recognition is a personalized selection of invariant features in humans, not simply explained by hierarchical feed-forward vision models H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour - Scientific reports, 2017
99. Hard-wired feed-forward visual mechanisms of the brain compensate for affine variations in object recognition H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour - Neuroscience, 2017
100. 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)
101. Average activity, but not variability, is the dominant factor in the representation of object categories in the brain H Karimi-Rouzbahani, N Bagheri, R Ebrahimpour - 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: 90-107Nasour 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**.

11. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, "Compact hardware implementation of Keccak Hash Function", NCNIEE, 2013 (in Persian).
12. 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, **IEEE**.
13. 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**.
14. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, Ali Mahani "On the Security of RFID AntiCloning Security Protocol(ACSP)", ICACM'12, 2012, **IEEE**.
15. 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.
16. 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**.
17. 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**.
18. Nasour Bagheri, Reza Ebrahimpour, Amir Ghorab, Maryam Kamarzarin, "Compact hardware implementation of MIBS block cipher", IKT, 2012 (in Persian).
19. 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**.
20. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi "Cryptanalysis of Chen et al.'s RFID Access Control Protocol", Internet Technology and Secured Transactions (ICITST), 2011, **IEEE**.
21. 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.
22. 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**.
23. 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.
24. Praveen Gauravaram, Lars R. Knudsen, Nasour Bagheri, Lei Wei" Improved Security Analysis of Fugue-256 (Poster)", ACISP 2011, **LNCS**, 428-432.
25. 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**.
26. 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.
27. N.Bagheri, M.Naderi, B.Sadeghiyan, M.Safkhani "Cryptanalysis of L-Pipe Hash Structure" 17th ICEE 2009, Tehran, Iran.

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