محمدرضا عارف

استاد ممتازدانشگاه صنعتی شریف

تلفن: ۶۶۱۶۵۹۳۵-۰۲۱

پست الکترونیک: aref@sharif.edu

سوابق تحصیلی:

- دکترا در رشته برق- مخابرات از دانشگاه استنفورد- ۱۳۵۹.
  - ✓ **عنوان رساله دکترا**: "Information Flow in Relay Networks"
- کارشناسی ارشد در رشته برق- مخابرات از دانشگاه استنفورد- ۱۳۵۵.
- کارشناسی در رشته برق- الکترونیک از دانشگاه تهران- ۱۳۵۴.

سوابق علمی:

- استاد ممتاز دانشگاه صنعتی شریف ۱۳۹۳- تاکنون
- پژوهشگر نمونه دانشگاه صنعتی شریف ۱۳۹۳
- استاد نمونه دانشگاه صنعتی شریف ۱۳۸۶
- استاد دانشگاه صنعتی شریف ۱۳۷۶- تاکنون
- استاد دانشگاه صنعتی اصفهان ۱۳۷۶- ۱۳۷۴
- استاد نمونه آموزش عالی کشور ۱۳۷۳
- دانشیار دانشگاه صنعتی اصفهان ۱۳۷۴- ۱۳۷۰
- استادیار دانشگاه صنعتی اصفهان ۱۳۷۰- ۱۳۶۱
- سرپرستی جمعاً ۱۸۶ رساله دکتری/ پایان‌نامه کارشناسی ارشد (۴۵ رساله دکتری و ۱۴۱ پایان‌نامه کارشناسی ارشد)
- راه‌اندازی دوره کارشناسی ارشد برق دانشگاه صنعتی اصفهان، دکترای برق دانشگاه صنعتی اصفهان و دکترای برق دانشگاه تربیت مدرس.
- مجری طرح های مختلف پژوهشی از جمله **طرح کلان ملی توسعه علم و فناوری رمز در کشور**

سوابق کاری:

- معاون طرح و توسعه شرکت مخابرات ایران ۱۳۶۰-۱۳۵۹
- معاون دانشجوئی وزارت فرهنگ و آموزش عالی ۱۳۶۱-۱۳۶۰
- معاون آموزشی وزارت فرهنگ و آموزش عالی۱۳۶۲-۱۳۶۱
- قائم مقام و معاون هماهنگی وزارت فرهنگ و آموزش عالی ۱۳۶۳-۱۳۶۲
- معاون آموزشی وزارت فرهنگ و آموزش عالی ۱۳۶۹-۱۳۶۸
- رئیس دانشگاه تهران ۱۳۷۶-۱۳۷۳
- وزیر پست و تلگراف و تلفن ۱۳۷۹-۱۳۷۶
- معاون رئیس جمهور و رئیس سازمان مدیریت و برنامه‌ریزی کشور ۱۳۸۰-۱۳۷۹
- معاون اول رئیس جمهور ۱۳۸۴-۱۳۸۰
- عضو مجمع تشخیص مصلحت نظام ۱۳۸۱- تاکنون
- عضو شورای عالی انقلاب فرهنگی ۱۳۷۸ – ۱۴۰۰
- عضو پیوسته فرهنگستان علوم جمهوری اسلامی ایران ۱۳۸۴- تاکنون
- رئیس انجمن رمز ایران ۱۳۷۹- ۱۳۹۹
- رئیس انجمن علمی کنترل و فرماندهی(C4I) ایران ۱۳۸۶- تاکنون
- رئیس انجمن علمی شبکه‌های هوشمند انرژی ایران ۱۳۹۱-۱۳۹۷
- رئیس گروه علوم مهندسی فرهنگستان علوم جمهوری اسلامی ایران ۱۳۸۸-۱۳۹۴
- رئیس کمیسیون پیشبرد ریاضیات کشور فرهنگستان علوم جمهوری اسلامی ایران ۱۳۹۱- تاکنون
- رئیس بنیاد پیشبرد علم و فناوری ایران (FAST- IRAN) ۱۳۸۸ - تاکنون
- رئیس کانون استادان دانشگاهی ۱۳۹۴- تاکنون
- رئیس بنیاد امید ایرانیان ۱۳۸۸– تاکنون
- نماینده مردم تهران در دوره دهم مجلس شورای اسلامی ۱۳۹۵– ۱۳۹۹

Publication:

کتاب‌های ترجمه شده:

۱. سیستم‌های مخابراتی دیجیتال و آنالوگ(ویرایش ۱ تا ۷).
۲. سیگنال‌ها و سیستم‌ها.
۳. سیگنال‌های تصادفی.

۴۴۹ مقاله شامل:

۱. تعداد مقالات انگلیسی چاپ شده در مجلات: ۱۶۵
۲. تعداد مقالات انگلیسی ارائه شده در کنفرانس‌ها: ۲۴۸
۳. تعداد مقالات فارسی چاپ شده در مجلات: ۱۳
۴. تعداد مقالات فارسی ارائه شده در کنفرانس‌ها: ۲۳

Journal Papers:

1- M. R. Aref, A. El-Gamal, "The Capacity of the Semi - Deterministic Relay Channel," IEEE Trans on; Inf. Theory, Vol. 28, May 1982.

2- Y. Zakeri, M. R. Aref, "Design Algorithms for Doppler and MTI Filters (Using Chebyshev Approximation)," Esteghlal Journal of Engineering No.9, March 1991.

3- G. Abed Hodtani, M. R. Aref, "Capacity Theorems for Relay Networks with Partial Feedback," Amirkabir Journal of Science and Technology, Vol.4, No.16, winter 1991.

4- M. R. Aref, Fackoor Yekta, "Interface Data Processing of RADAR," Amirkabir Journal of Science and Technology, Vol. 5, No. 20, Spring 1992.

5- M. R. Aref, F. Hendesi, M. Omoomi, "A New Fast Data Encryption Algorithm (FDE)," Isteghlal Journal of Engineering, No.11, Oct. 1992.

6- M. R. Aref, F. Hendesi, "New Exhaustive Search Attack to the DES," Iranian Journal of Engg., Vol.4, No.24, Fall 1993.

7- M. R. Aref, M. Soliemanipour, "The Capacity of Two Hopfield Network and A Practical Way To Increase Its Memory," Memoirs Of the Faculty of Engineering University of Tehran, No. 53, Dec. 1993.

8- M. R. Aref, M. Berenjkoob, "A Fast Coding Algorithms For Vector Quantization," Amirkabir Journal of Science and Technology, Vol. 6, No.24, winter 1994.

9- M. Modarres-Hashemi, M. R. Aref, "The Linear Complexity of the Universal Logic Sequence," Scientia Iranica, Vol.2, No.1, Spring 1995.

10- M. M. Nayebi, M. R. Aref, M. H. Bastani, "Detection of Coherent Radar Signals with Unknown Doppler Shift," IEE Proc. Radar, Sonar, and Navigation Vol.143, No.2, April 1996.

11- Taban, M. R. Aref, Alavi, M. M. Nayebi, "A New Approach for Coherent Radar Detection in K- Dist. Interberence," Scientia Iranica, Vol.5, No.1&2, Spring, 1998.

12- A. Sheykhi, M. M. Nayebi, M. R. Aref, "Adaptive Detection Algorithm for Radar Signal AR Interference," IEE Proc. Radar, Sonar Navigation, Vol. 45, No.5, Oct. 1998.

13- A. Sheykhi, M. M. Nayebi, M. R. Aref, "Adaptive Detection Algorithms for Radar Signals in Auto-Regressive Interference," IEE Proc. Radar, Sonar, and Navigation, Vol.145, No.5, Oct. 1998.

14- M. Dakhilalian, M. R. Aref, B. Sadeghian, M. M. Modarres-Hashemi, "A New Statistical Test Based on Linear Complexity Profile (LCP)," Amirkabir Journal of Science of Technology, Vol.11, No. 42, pp.67-73, Tehran, Iran, 1999..

15- G. H. Mirjalili, M. R. Aref, M. M. Nayebi, M. Kahrizi, "Adaptive Decision Fusion in Detection Networks," Esteghlal Journal of Engg. Vol.19, No.1, Sept., 2000.

16- M. Berenjkoub, H. Saeidi, M. R. Aref, "The Kryptoknight Family of Protocols Evaluation and Enhancement," Scientia Iranica, Vol.7, No.3&4, Oct. 2000.

17- F. Ashtiani, J. A. Salehi, M. R. Aref, "A New General and Flexible Model for CDMA Cellular Networks," Scientia Iranica, 2002.

18- F. Ashtiani, J. A. Salehi, M. R. Aref, "Mobility Modeling and Analytical Solution for Spatial Traffic Distribution in Wireless Multimedia Networks," IEEE JSAC-Vol.21-No.10, Dec. 2003.

19- F. Ashtiani, J. A. Salehi, M. R. Aref, "A Flexible Dynamic Traffic Model for Reverse Link CDMA Cellular Network," IEEE Trans. Wireless Communication, Vol. 3, No .1, Jan 2004.

20- F. Ashtiani, M. R. Aref, J. A. Salehi, "Performance Comparison of Admission control Policies for New Cells in Soft-Handoff Regions for CDMA Cellular Networks," Scientia Iranica Vol. 11, No. 3, Summer 2004.

21- H. Rohi, M. R. Aref, M. E. Kalantari, "Capacity Analysis for a CDMA Cellular System with Mixed Cell Sizes and Imperfect Power Control," Scientia Iranica, Vol. 11, No .3, Summer 2004.

22- M. Derakhtian, A. A. Tadaion, M. M. Nayebi, M. R. Aref, "Detection of a Sinusoid Signal with Unknown Parameters Using Wavelets," Proc. IEE Waveform, Diversity and Design, Nov. 2004.

23- A. Payandeh, M. Ahmadian, M.R. Aref, "A Secure Error-Resilient Lossless Source Coding Scheme Based On Punctured Turbo Codes" Iranian J. of Elec. & Comput. Engg. , Vol.5, No.1, Winter-Spring 2006.

24- A. Payandeh, M. Ahmadian, M.R. Aref, "Adaptive Secure Channel Coding Based on Punctured Turbo Codes," IEE Proc. Communication, Vol.153, No.2, April 2006.

25- A. Payandeh, M. Ahmadian, M. R. Aref, "An Adaptive Secure Channel Coding Scheme for Data Transmission Over the LEO Satellite Channel," Scientica Iranica, Vol.13, No.4 , Oct. 2006.

26- A. A. Tadaion, M. Derakhtian, S. Gazor, M. Nayebi, M.R. Aref, "Signal Activity Detection of PSK Signals," IEEE Trans. on Comm., Vol. 54, No.8, Aug. 2006.

27- A. A. Tadaion, M. Derakhtian, S. Gazor, M.R. Aref, "A Fast Multiple Source Detection and Localization Array Signal Processing Algorithm Using the Spatial Filtering and ML Approach," IEEE Trans. on Signal Processing , Vol.55 , No.5 , May 2007.

28- M. Derakhtian, A.A. Tadaion, M.M. Nayebi, M.R. Aref, "Detection of a Band-Limited Signal Using an Orthonormal Fully-Decimated Filter-Bankh," Scientia Iranica, Vol. 14, No. 6, Dec. 2007, pp. 555-565.

29- M. R. Taban, M. R. Aref, "A New Approach for Coherent Radar Detection in Pseudo-Gaussian Interference," Modares Journal, No. 26, Winter 2007, pp. 31-44.

30- F. Haddadi, M.M. Nayebi, M.R. Aref, "On The Positive Definiteness of Polarity Coincidence Correlation Coefficient Matrix," IEEE Signal Processing Letters, Vol. 15, No. 1, Jan. 2008, pp. 73-76.

31- B. Bahrak, M. R. Aref, "Impossible Differential Attack on 7-round AES-128," IET J. on Information Security, Vol. 2, No. 2, Feb. 2008, pp. 28-32.

32- L. Ghabeli, M.R. Aref, "A New Achievable Rate and the Capacity of Some Classes of Multilevel Relay Network," EURASIP Journal on Wireless Communications and Networking, doi: 10.1155/2008/135857, 2008.

33- A. A. Tadaion, M. Derakhtian, M.M. Nayebi, M.R. Aref, "GLR Detector for Coded Signals in Noise and Interference," Scientia Iranica, Vol. 15, No. 2, pp. 170-174, April 2008.

34- L. Ghabeli, M R. Aref, "Symmetric Relaying Strategy for Two-Relay Networks," IEEE Communications Letters, Vol. 12, No. 10, Oct. 2008, pp. 708-710.

35- L. Ghabeli, M.R. Aref, "Symmetric Relaying Based on Partial Decoding and the Capacity of a Class of Relay Networks," IET Communications, Vol. 3, No. 1, Jan. 2009, pp. 151-159.

36- A. Sobhiafshar, T. Eghlidos, M.R. Aref, "Efficient Secure Channel Coding Based on Quasi-cyclic Low- density-Parity-check Codes," IET Communications, Vol. 3, No. 2, Feb. 2009, pp. 279- 292.

37- F. Haddadi, M.M. Nayebi, M.R. Aref, "Direction-of-Arrival Estimation for Temporally Correlated Narrowband Signals," IEEE Trans. on Signal Processing, Vol. 57, No. 2, Feb. 2009, pp. 600-610.

38- L. Ghabeli, M.R. Aref, "Comprehensive Partial Decoding Approach for Two-Level Relay Networks," IET Communications, Vol. 3, No. 4, April 2009, pp. 585-596.

39- L. Ghabeli, M. R. Aref, "Symmetric Semideterministic Relay Networks With No Interference at the Relays," in IEEE Trans. on Inf. Theory, Vol. 57, No. 9, 2011.

40- A. Farhadian, M. R. Aref, "Efficient Method for Simplifying and Approximating the S-Boxex Based on Power Functions," IET Information Security, Vol. 3, No.3, pp.114-118, Sept. 2009.

41- G. A. Hodtani, M.R. Aref, "New Achievable Rate and A Certain Capacity Result for A Stochastic Two Relay Network with No Interference," IET Communications, Vol. 3, No. 7, July 2009, pp. 1153- 1162.

42- G. A. Hodtani, M. R. Aref, "On the Devroye-Mitran-Tarokh Rate Region for the Cognitive Radio Channel," IEEE Trans. on Wireless Communications, Vol. 8, No. 7, pp. 3458- 3461, July 2009.

43- G. A. Hodtani, M. R. Aref, "Unified Approach to the Capacity Evaluation of the Relay Channel," IET Communications, Vol.3, No. 7, pp. 1208- 1215, July 2009.

44- S. Saleh Kalaibar, L. Ghabeli, M. R. Aref, "An Achievable Rate Region for Multiple-Access-Relay- Networks," IET Communications, Vol. 4, No. 15, pp. 1792- 1798, 2010.

45- A. Payandeh, M. Ahmadian, M. R. Aref, "Source Coded Modulation for Discrete Sources With Memory," Sharif Journal, No. 52, pp. 31-36, 2010.

46- F. Haddadi, M.M. Nayebi, M.R. Aref, "Statistical Performance Analysis of Detection of Signals by Information Theoretic Criteria," IEEE Transactions on Signal Processing, Vol. 58, No. 1, pp.452-457, Jan 2010.

47- A. H. Salavati, B.H. Khalaj, P. Crespo, M.R. Aref, "Wireless QoSNC A Novel Approach to QoS-based Network Coding in Wireless Networksa," J. of Communications and Networks, Vol.12, NO.1, pp. 86- 94, Jan 2010.

48- B. Akhbari, M. Mirmohseni, M. R. Aref, "Compress-and-Forward Strategy for Relay Channel with Causal and Non- Causal Channel State Information," IET Communications, Vol. 4, No. 10, pp. 1174- 1186, July 2010.

49- S. Saleh- Kalaibar, L. Ghabeli, M. R. Aref, "An Achievable Rate for Relay Networks Based on Compress-and-Forward Strategyn," IEEE Communications Letters, Vol. 14, No.4, pp. 279-281, April 2010.

50- S. Saleh- Kalaibar, L. Ghabeli, M. R. Aref, "Achievable Rate Region for Broadcast-Relay Networks with Two Cooperative Relays," IET Communications, Vol. 4, No.8, pp.946- 955, May 2010.

51- B. Akhbari, M. Mirmohseni, M. R. Aref, "Compress- and- Forward Strategy for Relay Channel With Causal and Non-Causal Channel State Information," IET Communications, Vol. 4, No. 10, pp.1174- 1186, Oct 2010.

52- A. Sharifi, E. Mehrabi, T. Eghlidos, M. R. Aref, "Algebraic Attacks from a Groebner Basis Perspective," International Journal of Algebra, Vol. 4, No. 10, pp. 447-459, Oct 2010.

53- S.Salimi, M. Salmasizadeh, M. R. Aref, "Generalized Secure Distributed Source Coding with Side Information," IET Communications, Vol. 4, No. 18, pp. 2262- 2272, 2010.

54- L.Ghabeli, M. R. Aref, "Capacity of a Class of Relay Network with Orthogonal Component," IET Communications, Vol. 4, No. 18, pp. 2181- 2186, 2010.

55- N. Rohani, Z. Noferesti, J. Mohajeri. M. R. Aref, "Guess and Determine Attack on Biviumnent," Journal of Information Processing Systems, Vol. 7, No.1, pp. 151-156, Jan. 2011.

56- S. Salimi, M. Salmasizadeh, M. R. Aref, "Rate Regions of Secret Key Sharing in a New Source Model," IET Communications, Vol. 5, No. 4, pp. 443-455, 2011.

57- M. H. Yassaee, M. R. Aref, "Slepian-Wolf Coding Over Cooperative Relay Networksl," IEEE Trans. on Inf. Theory, Vol. 57, No.6, pp. 3462- 3482, June 2011.

58- M. Mirmohseni, B. Akhbari, M. R. Aref, "On the Capacity of Interference Channel with Causal and Non-causal Generalized Feedback at the Cognitive Transmitter," IEEE Transaction on Information Theory, Vol. 58, No.5, pp. 2813-2837, May 2012.

59- B. Akhbari, R. Khosravi, M. R. Aref, "Cooperative relay broadcast channels with partial causal state information," IET Communications, Vol. 5, No. 6, pp.760- 774, 2011.

60- S. Salimi, M. Salmasizadeh, M. R. Aref, "Key Agreement Over Multiple Access Channel," IEEE Trans. on Info. Forensics and Security, Vol.6, No.3, pp.775-790, 2011.

61- A. Haghi, R. Khosravi farsani, M. R. Aref, F. Marvasti, "The Capacity Region of p-Transmitter/q- Receiver Multiple-Access Channels with Common Information," IEEE Trans. on Info. Theory, Vol.57, No.11, Nov.2011, pp. 7359-7376.

62- M. Mirmohseni, B. Akhbari, M. R. Aref, "Capacity Regions for Some Classes of Multiple Access-Cognitive Interference Channel," EURASIP Journal on Wireless Communications and Networking, Nov. 2011.

63- M. Mirmohseni, B. Akhbari, M. R. Aref, "Compress-and-Forward Strategy for Cognitive Interference Channel with Unlimited Look-Ahead," IEEE Communications Letters, Vol. 15, No.10, pp1068- 107, Oct. 2011.

64- R. Aghajani, R.Saadat, M.R.Aref, G.Mirjalili, "Symbol Error Rate Analysis and Power Allocation forIncremental- Selective Decode-and- Forward Cooperative Communications Over Fading Channels," IET Communications, 2012.

65- P. Babaheidarian, S. Salimi, M. R. Aref, "Simultaneously Generating Multiple Keys in a Four-Terminal Network," IET Info. Security, 2012.

66- M. J. Emadi, M. Zamani ghomi, M. R. Aref, "Multiple Access Channel with Correlated States and Cooperating Encoders," IET Communications, Vol. 6, No. 13, pp. 1857-1867, Sept. 2012.

67- M. R. Alaghband, M. R. Aref, "Dynamic and Secure Key Management Model for Hierarchical Heterogeneous Sensor Networks," IET Information Security, Vol. 6, No.4, pp. 271-280, Dec. 2012.

68- R. hooshmand, T. eghlidos, M. R. Aref, "Improving the Rao-Nam secret key cryptosystem using regular EDF-QC-LDPC codes," ISeCure, 2012.

69- M. Mirmohseni, B. Akhbari, M. R. Aref, "Three-User Cognitive Interference Channel Capacity Region with Strong Interference," IET Communications, Vol. 6, No. 13, 2012.

70- M. Alagheband, M. R. Aref, "Unified Privacy Analysis of New-Found RFID Authentication Protocols," Security and Communication Networks, 2012.

71- F. Farhat, A. Diyanat, S. Ghaemmaghami, M. R. Aref, "Eigenvalues-based LSB Steganalysis," ISeCure, Vol. 4, No. 2, pp. 97-106, 2012.

72- Z. Ahmadian, M. Salmasi zadeh, M. R. Aref, "Desynchronization Attack on RAPP Ultralightweight Authentication Protocol," Information Processing Letters, Vol. 113, No. 7, pp. 205-209, April 2013.

73- Z. Ahmadian, M. Salmasi zadeh, M. R. Aref, "Recursive Linear and Differential Cryptanalysis of Ultralightweight Authentication Protocols," IEEE Transaction on Information Forensics and Security, Vol. 8, No. 7, July 2013.

74- S. Salimi, Mikael Skoglund, Jovan Dj Golic, M. Salmasi zadeh, M. R. Aref, "Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback," IEEE Journal on Selected Areas in Communications, Vol. 31, No. 9, Sept. 2013.

75- R. Aghajani, R. Saadat, M. R. Aref, "Power Allocation and Performance Analysis for Incremental- Selective Decode-and-Forward Cooperative Communications over Nakagami-m Fading Channels," IEICE Trans. Commun, Vol. E96-B, No. 6, Jun. 2013.

76- S. Saleh-Kalaibar, M. Mirmohseni, M. R. Aref, "One-Receiver, Two-Eavesdropper Broadcast Channel with Degraded Message Sets," IEEE Transactions on Information Forensics and Security, Vol. 8, No. 7, pp. 1162-1172, 2013.

77- M. Rahimi, M. Barmshory, M. H. Mansouri, M. R. Aref, "Dynamic Cube Attack on Grain-v1," IET Information Security, 2013.

78- H. Sedghi, M. R. Pakravan, M. R. Aref, "A Misbehavior-Tolerant Multipath Routing Protocol for Wireless Ad hoc Networks," International Journal of Wireless Information Networks, Vol.2, No. 2, pp.6-15, 2013.

79- M. J. Emadi ،A. G. Davoodi, M. R. Aref, "Analytical Power Allocation for a Full Duplex Decode-and-Forward Relay Channel," IET Communications, Vol. 7, No. 13, pp. 1338-1347, Sept. 2013.

80- M. R. Alagheband, M. R. Aref, "Simulation-based Traceability Analysis of RFID Authentication Protocols," Wireless Personal Communications, vol.77, no.2, pp. 1019-1038, 2014.

81- S. Salehkalaibar, M. R. Aref, "Physical layer security for some classes of three-receiver broadcast channels," IET Communications, Vol. 8, No.11, pp. 1965-1976, July 2014.

82- M. H. Yassaee, M.R. Aref, A. Gohari, "Achievability Proof via Output Statistics of Random Binning," IEEE Transactions on Information Theory, Vol. 60, No. 11, 2014.

83- S. Ahmadi, Z. Ahmadian, J. Mohajeri, M. R. Aref, "Biclique Cryptanalysis of Block Ciphers LBlock and TWINE with Practical Data Complexity," Journal of Systems and Software, 2014.

84- M. Bayat, M. Pournaghi, M. Barmshoory, M. Rahimi, M. Gardeshi, M. R. Aref, "NERA: A Novel and Efficient RSU Based Authentication Scheme for VANETs," Security and Communication Networks, 2014.

85- N. Ardalani, M. Mirmohseni, M. R. Aref, "Three-User Interference Channel with Common Information: A Rate Splitting Based Achievability Scheme," IET Communications, Vol. 8, No. 4, pp. 462-470, March 2014.

86- M. Fatemi, R. Ghasemi, T. Eghlidos, M. R. Aref, "Efficient multistage secret sharing scheme using bilinear map," IET Information Security, Vol. 8, No. 4, pp. 224-229, July 2014.

87- M. J. Emadi, M. Nasiri Khormuji, M. Skoglund, M. R. Aref, "Multi-layer Gelfand-Pinsker Strategies for the Generalised Multiple-Access Channel," IET Communications, Vol. 8, No. 8, pp. 1296-1308, May 2014.

88- H. Ghasemzadeh, A. payandeh, M. R. Aref, "Toward an Energy Efficient PKC-Based Key Management System for WSNs," ISeCure, 2014.

89- S. Ahmadi, Z. Ahmadian, J. Mohajeri, M. R. Aref, "Low Data Complexity Biclique Cryptanalysis of Block Ciphers with Application to Piccolo and HIGHT," IEEE Transactions on Information Forensics and Security, Vol.9, Issue 10, pp. 1641-1652, 2014.

90- Behzad Abdolmaleki, Hamidreza Bakhshi, Karim Bagheri, Mohammad Reza Aref, "Analysis of an RFID Authentication Protocol in Accordance with EPC Standards," International Journal of Information & Communication Technology Research (IJICTR), Vol. 6, No. 4, pp. 7-12, Autumn 2014.

91- N. Bagheri, J. Alizadeh, M. R. Aref, "Artemia: A Family of Provably Secure Authenticated Encryption Schemes," ISeCure, Vol. 6, No. 2, pp. 125-136, 2014.

92- S. Salehkalaibar, M. R. Aref, "Lossy Transmission of Correlated Sources over Multiple-Access Wiretap Channels," IET Communications, Vol. 9, No. 6, pp. 754-770, April 2015.

93- M. Ehdaie, N. Alexiou, M. Attari, M. R. Aref, P. Papadimitratos, "Key splitting: making random key distribution schemes resistant against node capture," Security and Communication Networks, Vol. 8, No. 3, pp. 431-445, Feb. 2015.

94- M. Bayat, H. R. Arkian, M. R. Aref, "A Revocable Attribute Based Data Sharing Scheme Resilient to DoS Attacks in Smart Grid," Wireless Netwoks, Vol. 21, No. 3, April 2015.

95- M. Bayat, M. R. Aref, "An Attribute Based Tripartite Key Agreement Protocol," International Journal of Communication Systems, Vol. 28, No. 8, pp. 1419-1431, May 2015.

96- Seyed Mohammad Alavi, Karim Baghery, Behzad Abdolmaleki, Mohammad Reza Aref, "Traceability Analysis of Recent RFID Authentication Protocols," Wireless Personals Communications, Vol. 83, No. 3, pp. 1663-1682, August 2015.

97- Z. Ahmadian, M. Salmasizadeh, M. R. Aref, "Biclique Cryptanalysis of the Full-Round KLEIN Block Cipher," IET Information Security, Vol. 9, No. 5, pp. 294-301, 2015.

98- Mohammad Yassaee, Amin Gohari, Mohammad Reza Aref, "Channel Simulation via Interactive Communications," IEEE Transactions on Information Theory, Vol. 61, No. 6, pp. 2964-2982, 2015.

99- Reza Hooshmand, Mohammad Reza Aref, and Taraneh Eghlidos, "Secret Key Cryptosystem based on Non-Systematic Polar Codes," Wireless personal Communications, 27 May 2015.

100- Hamid Ghanizade Bafghi, Babak Seyfe, Mahtab Mirmohseni, Mohammad Reza Aref, "Capacity of Channel with Energy Harvesting Transmitter," IET Communications, Vol. 9, No. 4, pp. 526-531, March 2015.

101- Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, Mohammad Reza Aref, "Enhancing Privacy of Recent Authentication Schemes for Low-Cost RFID Systems," ISeCure, Vol. 7, No. 2, 2015.

102- Reza Hooshmand, Mohammad Reza Aref, and Taraneh Eghlidos, "Physical Layer Encryption Scheme Using Finite-Length Polar Codes," IET Communications, ol. 9, No. 15, pp. 1857-1866, Oct. 2015.

103- Javad Alizadeh, Mohammad Reza Aref, Nasour Bagheri, Hassan Sadeghi, "Cryptanalysis of Some First Round CAESAR Candidates, ISeCure, Vol. 7, No. 2, 2015.

104- Masoumeh Koochak Shooshtari, Thomas Johansson, Mahmoud Ahmadian-Attari, Mohammad Reza Aref, "Cryptanalysis of McEliece cryptosystem variants based on QC-LDPC Codes," IET Information Security, Vol. 10, No. 4, pp. 194-202, July, 2016.

105- Hassan Zivari-Fard, Bahareh khbari, Mahmoud Ahmadian-Attari, and Mohammad Reza Aref, "Imperfect and Perfect Secrecy in Compound Multiple Access Channel with Confidential Message," IEEE Transactions on Information Forensics & Security, Vol. 11, No. 6, pp. 1239-1251, Jan. 2016.

106- Carl Löndahl, Thomas Johansson, Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari, Mohammad Reza Aref, "Squaring Attacks on McEliece Public-key Cryptosystems Using Quasi-cyclic Codes of Even Dimension," Designs, Codes and Cryptography, Vol. 80, No. 2, pp. 359-377, Aug. 2016.

107- Hassan Zivari-Fard, Bahareh Akhbari, Mahmoud Ahmadian-Attari, Mohammad Reza Aref, "Multiple Access Channel with Common Message and Secrecy constraint," IET Communications, Vol. 10, No. 1, pp. 98-110, Feb. 2016.

108- Hamid G. Bafghiy, Babak Seyfey, Mahtab Mirmohseniz, Mohammad Reza Aref, "On The Secrecy of the Cognitive Interference Channel with Partial Channel States," Transactions on Emerging Telecommunications, Vol. 27, No. 11, pp. 3739-3753, 2016.

109- Farzin Haddadpour, Mohammad Hossein Yassaee, Salman Beigi, Amin Gohari1, and Mohammad Reza Aref, "Simulation of a Channel with Another Channel," IEEE Transactions on Information Theory, Vol. 63, No. 5, pp. 2659-2677, 2016.

110- Masoumeh Koochak Shooshtari, Mahmoud Ahmadian-Attari and Mohammad Reza Aref, "Provably secure strong designated verifier signature scheme based on coding theory," International Journal of Communications Systems, , Vol. 30, No. 7, pp. e3162, 2017.

111- Mohammad Zare Ahangarkolaei, Seyed Reza Hoseini Najarkolaei, Siavash Ahmadi and Mohammad Reza Aref, "Zero Correlation Linear Attack on Reduced Round Piccolo-80," IEEE Transactions on Information Theory, Submitted.

112- Sadaf Salehkalaibar, Amin Gohari and Mohammad Reza Aref, "Man-In-The-Middle Attack: An Information Theoretic Perspective," Transactions on Information Forensics &Security, Submitted.

113- Milad Rezaee, Mahtab Mirmohseni, Mohammad Reza Aref, "Energy Harvesting Systems with Continuous Energy and Data Arrivals: the Optimal Offline and a Heuristic Online Algorithms," IEEE Journal on Selected Areas in Communications, Vol. 34, No. 12, 2016.

114- Zahra Ahmadian, Mahmoud Salmasizadeh, Mohammad Reza Aref, "An Improved Truncated Differential Cryptanalysis of Klein," Tatra Mountains Mathematical Publications Journal, pp. 135-147, 2016.

115- Behzad Karim Baghery, Shahram Khazaei, Mohammad Reza Aref, "Game-Based Privacy Analysis RFID Security Schemes for Confident-spacing:Authentication IoT," Wireless Personal Communication, Vol. 95, No. 4, pp. 5057-5080, 2017.

116- Milad Johnny, Mohammad Reza Aref, "An Efficient Precoder Size for Interference Alignment of the K-user Interference Channel," IEEE Communications Letters, Vol. 21, No. 9, pp. 1941-1944, 2017.

117- Majid Bayat, Mohammad Beheshti Atashgah, Mohammad Reza Aref, "A Secure and Efficient Chaotic Maps Based Authenticated Key-Exchange Protocol for Smart Grid," Wireless Personal Communications, Vol. 97, No. 2, pp. 2551-2579, 2017.

118- Mahdi Mojahedian, M. R. Aref, Amin Amin Zadeh, "Perfectly Secure Index Coding," IEEE Transactions on Information Theory, Vol. 63, No. 11, pp. 7382-7395, 2017.

119- Reza Hooshmand, and Mohammad Reza Aref, “Polar Code-based Secure Channel Coding Scheme with Small Key Size,” IET Communications, Vol. 11, No. 15, pp. 2357-2361, 2017.

120- Reza Hooshmand, Mohammad Reza Aref, "Efficient Polar Code-based Physical Layer Encryption Scheme," The IEEE Wireless Communications Letters, Vol. 6, No. 6, pp. 710-713, 2017.

121- Milad Rezaee, Mahtab Mirmohseni, Mohammad Reza Aref, “On Optimal Online Algorithms for Energy Harvesting Systems with Continuous Energy and Data Arrivals,” IEEE Wireless Communications Letters, Vol. 6, No. 3, pp. 286-289, 2017

122- Z. Salami, M. Ahmadian-Attari, H. Jannati & M.R. Aref, "A Location Privacy-Preserving Method for Spectrum Sharing in Database-Driven Cognitive Radio Networks", Wireless Personal Communications, Vol. 95, No. 4, pp. 3687-3711, 2017.

123- Arash Azimi, S. Ahmadi, Jawad Mohajeri, Mohammad Reza Aref, “Improved Impossible Differential and biclique cryptanalysis of hight,” International Journal of Communication Systems, Vol. 31, No. 1, 2017.

124- B Mafakheri, T Eghlidos, H Pilaram, "An Efficient Secure Channel Coding Scheme based on Polar Codes", ISeCure, Vol. 9 No. 2, pp.13-20, 2017.

125- M Ehdaie, N Alexiou, M Ahmadian, MR Aref, P Papadimitratos, "Mitigating Node Capture Attack in Random Key Distribution Schemes through Key Deletion", Journal of Communication Engineering, Vol. 6, No. 2, pp. 99-109, 2017.

126- R Hooshmand, MR Aref, "Public key cryptosystem based on low density lattice codes", Wireless Personal Communications, Vol. 92, No. 3, 1107-1123, 2017/2/1.

127- E Vahedi, M Bayat, MR Pakravan, MR Aref, "A secure ECC-based privacy preserving data aggregation scheme for smart grids", Computer Networks, Vol. 129, pp. 28-36, 2017.

128- M Rezaee, M Mirmohseni, V Aggarwal, MR Aref, "Optimal Transmission Policies for Multi-hop Energy Harvesting Systems," IEEE Transactions on Green Communications and Networking, Vol. 2, No. 3, pp. 751-763, Sept. 2018.

129- M. R. Asaar, M. Salmasizadeh, M. R. Aref, "A provably secure code-based short signature scheme and its nontransferable variant", International Journal of Communication Systems, Vol. 31, No. 6, pp. e3519, 2018.

130- M. Johnny and M. R. Aref, “Blind interference alignment for the K –User SISO interference channel using reconfigurable antennas”, IEEE Communications Letters, vol. 22, no. 5, pp. 1046 - 1049, Mar. 2018.

131- M. R. Asaar, M. H. Ameri, M. Salmasizadeh & M. R. Aref, “A provably secure code-based concurrent signature scheme”, IET Information Security, Vol. 12, No. 1, pp. 34-41, 2018.

132- MM Oliaee, M Delavar, MH Ameri, J Mohajeri, MR Aref, "On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets", ISeCure, Vol. 10, No. 2, 2018.

133- Mohammad Mahdi Mojahedian, Salman Beigi, Amin Gohari, Mohammad Hossein Yassaee, Mohammad Reza Aref, " A Correlation Measure Based on Vector-Valued L_p-Norms ", IEEE Transactions on Information Theory, Vol. 65, No. 12, p.p. 7985-8004, 2019/8/23.

134- M. Johnny and M. R. Aref, "A Multi-layer Encoding and Decoding Strategy for Binary Erasure Channel", IEEE Transactions on Information Theory, Vol. 65, No. 7, pp. 4143-4151, 2019.

135- R. Rabaninejad, M. Ahmadian Attari, M. R. Asaar, M. R. Aref, "Comments on a lightweight cloud auditing scheme: Security analysis and improvement ", Journal of Network and Computer Applications, Vol. 139, p.p. 49-56, 2019.

136- M Bayat, M Barmshoory, SM Pournaghi, M Rahimi, Y Farjami, M R Aref, "A new and efficient authentication scheme for vehicular ad hoc networks", Journal of Intelligent Transportation Systems: Technology, Planning, and Operations, Vol. 24, No. 2, p.p. 171-183, Published online: 04 Jul 2019.

137- A Akbarzadeh, M Bayat, B Zahednejad, A Payandeh, MR Aref, "A lightweight hierarchical authentication scheme for internet of things", Journal of Ambient Intelligence and Humanized Computing, Vol. 10, No. 7, p.p. 2607-2619, 2019.

138- M Johnny, MR Aref, F Razzazi, "Effect of unitary transformation on Bayesian information criterion for source numbering in array processing", IET Signal Processing, Vol. 13, No. 7, p.p. 670-678, 2019.

139- M Abolpour, M Mirmohseni, MR Aref, "On the Secrecy Performance of NOMA Systems with both External and Internal Eavesdroppers", arXiv preprint arXiv:1906.03929, 2019.

140- S Ahmadi, Z AHMADIAN, J MOHAJERI, MR AREF, "Biclique Cryptanalysis of Block Ciphers LBlock and TWINE-80 with Practical Data Complexity", THE ISC INTERNATIONAL JOURNAL OF INFORMATION SECURITY, Vol. 11, No.100464, p.p. 57-74, 2019

141- K Baghery, B Abdolmaleki, S Khazaei, MR Aref, "Breaking anonymity of some recent lightweight RFID authentication protocols", Wireless Networks, Vol. 25, No. 3, p.p. 1235-1252, 2019.

142- S Karimani, Z Naghdabadi, T Eghlidos, MR Aref, "An LWE-based verifiable threshold secret sharing scheme", Математические вопросы криптографии, Vol. 10, No. 2, p.p. 97-106, 2019.

143- R Rabaninejad, M Ahmadian, MR Asaar, M reza Aref, "A Lightweight Auditing Service for Shared Data With Secure User Revocation in Cloud Storage ", IEEE Transactions on Services Computing, Publication date 2019/5/28.

144- R Rabaninejad, MR Asaar, MA Attari, MR Aref, "An identity-based online/offline secure cloud storage auditing scheme", Cluster Computing, 1-14, 2019/11/6.

145- M Bayat, M Beheshti Atashgah, M. Barari, M R Aref, "Cryptanalysis and Improvement of a User Authentication Scheme for Internet of Things Using Elliptic Curve Cryptography", International Journal of Network Security, First Online: 2019/06/16.

146- M Johnny, MR Aref, "BIA for the K-user Interference Channel Using Reconfigurable Antenna at Receivers", IEEE Transactions on Information Theory, 2019/12/9.

147- S Ahmadi, MR Aref, "Generalized Meet in the Middle Cryptanalysis of Block Ciphers with an Automated Search Algorithm", IEEE Access, 2019/12/24.

148- M Niknam, S. Sadeghi, M R Aref, "Investigation of Some Attacks on GAGE (v1), InGAGE (v1), (v1.03), and CiliPadi (v1) Variants", ISeCure, Vol. 12, No. 1, p.p. 1-11, Jan. 2020.

149- R. Rabaninejad, M. Ahmadian Attari, M. Rajabzadeh Asaar, and M. R. Aref, "A lightweight identity-based provable data possession supporting users' identity privacy and traceability", Journal of Information Security and Applications, Vol. 51, 2020.

150- M Johnny, MR Aref, F Razzazi, "Corrigendum: Effect of unitary transformation on Bayesian information criterion for source numbering in array processing", IET Signal Processing, Vol. 14, No. 1, 13 February 2020.

151- R Hooshmand, MK Shooshtari, MR Aref, "PKC-PC: a variant of the McEliece public key cryptosystem based on polar codes", IET Communications, 2020/4/6.

152- S Ahmadi, MR Aref, "New Fixed Point Attacks on GOST2 Block Cipher", ISeCure, Vol. 11, No. 2, PP. 145-158, 2019.

153- M Bayat, Z Zare Jousheghani, A Kumar Das, P Singh, S Kumari, MR Aref, "A Lightweight Privacy-preserving Authenticated Key Exchange Scheme for Smart Grid Communications ", ISeCure, Vol. 11, No. 2, PP. 113-128, 2019.

154- P. Forghani, M. K. Shooshtari, MR. Aref, "PolarSig: An Efficient Digital Signature Based on Polar Codes", IET CommunicationsVol. 14, No. 17, PP. 2889-2897, 2020.

155- M Beheshti-Atashgaha, M R Arefb, M Barari, M Bayat, "Security and Privacy-preserving in e-health: a new framework for patient", Internet of Things, 2020/9/8.

156- R. Rabaninejad, M. Ahmadian Attari, M. Rajabzadeh Asaar, and M. R. Aref, "An Identity-Based Online/Offline Public Auditing Protocol in Cloud Storage", Cluster Computing, Vol. 23, PP. 1455-1468, 2020.

157- M Esfahani, H Soleimany, MR Aref, "Modified Cache-Template Attack on AES", Scientia Iranica, 2020/12/7.

158- R Sarenche, M Salmasizadeh, MH Ameri, MR Aref, "A secure and privacy-preserving protocol for holding double auctions in smart grid", Information Sciences 557, 108-129, 2021/5/1.

159- A. Norouzzadeh, R. Ramazani Khorshiddoust, M.R. Aref, "Determination of factors that affect the design of cryptographic algorithms by a cybernetic meta-model, validated with Q-analysis", Revista Ingenieria UC, Vol. 27, No. 1, Abril 2020.

160- M Johnny, MR Aref, "A MSWF root-MUSIC based on Pseudo-noise resampling technique", Electronics Letters, Vol. 57, No. 17, pp. 675-678, 2021/5/15.

161- A.M. Norouzzadeh, M.R. Aref and R. Ramazani Khorshid doust, "Analysis of Design Goals of Cryptography Algorithms based on Different Components", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 23, No. 1, 2021.

162- M. K. Shooshtari, M. R. Aref, "Smooth Projective Hash Function from Codes and Its Applications", IEEE Transactions on Services Computing, 2021/7/27.

163- M. Esfahani, H. Soleimany, A. M. Aref, "Enhanced Cache Attack on AES Applicable on ARM-based Devices with New Operating Systems", Computer Networks, Vol. 198, 2021/8/20.

164- AM Norouzzadeh Gil Molk, MR Aref, R Ramazani Khorshiddoust, "Leveled Design of Cryptography Algorithms Using Cybernetic Methods for Using in Telemedicine Applications", Computational Intelligence and Neuroscience, 2021/9/11.

165- M. Khaleghia, M. R. Aref, M. Rasti, "Comprehensive Comparison of Security Measurement Models", Journal of Applied Security Research, acceped, 2021/09/04.

166- Majid Bayat, Mohammad Beheshti, Morteza Barari, Mohammad Reza Aref, "A Secure Privacy-Preserving User Authentication Scheme for Internet of Things," Under Review in Journal of Supercomputing (SUPE).

167- Milad Johnny, Mohammad Reza Aref, "A Universal Encoding and Decoding Strategy for Binary Erasure Channel," Under Review in IEEE Wireless Communications Letters.

168- R. Rabaninejad, M. Ahmadian Attari, M. Rajabzadeh Asaar, and M. R. Aref, “Security Analysis and Improvement of a Public Shared-Data Auditing Protocol”, Under Review in IEEE Transactions on Cloud Computing.

169- R. Rabaninejad, M. Ahmadian Attari, M. Rajabzadeh Asaar, and M. R. Aref, “CoRPA: A Novel Efficient Shared Data Auditing Protocol in Cloud Storage”, Under Review in IEEE Transactions on Services Computing.

170- R. Rabaninejad, M. Rajabzadeh Asaar, M. Ahmadian Attari, and M. R. Aref, “On the Security of a Lightweight Cloud Data Auditing Scheme”, Under Review in Elsevier Journal of Network and Computer Applications.

Conference Papers:

1- F. Hendessi, M. R. Aref, "A Successful Attack against the DES," Proc. Third Canadian Workshop Springer- Verlog, LNCS 793-1, May 30-June 2, 1993.

2- H. Asghari, M. R. ARef, "The Use of LSP Frequencies in Speaker Recognition," Proc.ICSPAT-93- Santa Clara, Sept.28-Oct.1, 1993.

3- M. R. Aref, H. Asghari, "Speaker Identification Based on Instantaneous and Transitional LSP Frequencies," Proc.IEEE-ICT-94, Dubai, Jan.9-12, 1994.

4- M. M. Nayebi, M. R. Aref, "New Results in the Detection of Gaussian Signals in Gaussian Noise," Proc.IEEE-ICT-94, Dubai, Jan.9-12, 1994

5- Sayadian, M. Tabiani, M. R. Aref, "HSLSIN: Instantenous Normalization for Speaker Language Feature Extraction," Proc. ICSLP- 94, Japan, 1994.

6- Soleymanipour, M. R. Aref, Freeman, "On the Capacity of Neural Networks," Proc. Canadian Conf. on. E. E, Canada, 1994.

7- M. M. Nayebi, M. R. Aref, "Optimal Linear Detection of Gaussian Signals in Gaussian Noise," Proc. IEEE-ICT 94, Dubai, Jan 9-12, 1994

8- Sayadian, M. R. Aref, "Proposal and Implementation of a New and Powerful Algorithm for Determination of Pitch Frequency of Speech Signals," Proc.ICEE-94, Tarbiat Modarres University, Tehran, Iran, May 1994.

9- M. M. Nayebi, M. R. Aref, "Detection of Coherent Radar Signal with Unknown Doppler Shift in Noise," Proc.ICEE-94, Tarbiat Modarres University, Tehran, Iran, May 1994.

10- H. Asghari, M. R. Aref, "Speaker Recognition by Neural Networks Realization," Proc.ICEE-94, Tarbiat Modarres University, Tehran, Iran, May 1994.

11- M. Taban, M. R. Aref, "Different Methods for Generation of Stochastic Processes with Pseudo-Rayleigh Distributed Amplitude and Arbitrary Autocorrelation Function," Proc.ICEE-94, Tarbiat Modarres University, Tehran, Iran, May 1994.

12- M. R. Aref, M. M. Nayebi, "Likelihood Ratio Detection," IEEE ISIT-94, Trondheim, Norway, June 27-July 1, 1994.

13- M. R. Aref, M. M. Nayebi, "CALR and CGLR Algorithms for Detection of Radar Signals in Clutter," Proc. IS CR- 94, Japan, Nov 15-17, 1994.

14- M. R. Aref, H. Asghari, "A Feasibility Study on Applying Syllables as Basic Structures in Persian Speech Synthesis," Proc. IEEE-ICT-95, Bali, Indonesia, 1995.

15- Sayadian, M. Tabiani, M. R. Aref, "A New Pitch Synchronous Mel Scale Analysis for Feature Extraction of Spectral Envelope of Speech Signals," Proc. IEEE-ICT-95, Bali-Indonesia, 1995.

16- Hendessi, M. R. Aref, Gulliver, "Signature in Even Blocks: A Digital Signature Method Using DES," Proc. IEEE-ICC-95, Seattle, June 18, 1995.

17- M. M. Nayebi, M. R. Aref, "False Alarm and Detection Probabilities of Quadrature form Detectors," Proc. IEEE-ICT-96, Istanbul, Turkey, April 13-17, 1996.

18- M. R. Aref, Shah-Talebi, "Design of Causal Estimator filters for Nearly Cyclo-Stationary Processes," Proc.ICEE-96, University of Science & Technology, Tehran, Iran, May 1996.

19- Shah-Talebi, M. R. Aref, "Using Kalman Algorithm in Modifying Adaptive Weights of TSR-TDAF Structure," Proc. ICEE-96, University Of Science & Technology, Tehran, Iran, May 1996.

20- Payandeh, M. R. Aref, "Target Detection with Kalman Filtering," Proc.ICEE-96, University of Science & Technology, Tehran, Iran, May 1996.

21- M. R. Aref, Salamatian, "Consideration of Processing and Information Capacities for Structures," Proc.ICEE-96, University Of Science & Technology, Tehran, Iran, May 1996.

22- Refaeenia, M. R. Aref, "A Neural Algorithm for Designing Vector Quantization Code Book," Proc.ICEE-96, University Of Science & Technology, Tehran, Iran, May 1996.

23- Payandeh, M. R. Aref, "Detection of Neural Networks," Proc.ICEE-96, University Of Science & Technology, Tehran, Iran, May 1996.

24- Salamatian, M. R. Aref, "Examination of Neural Network Capabilities based on Information Theory," Proc. ICEE-96, University Of Science & Technology, Tehran, Iran, May 1996.

25- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Detection of Coherent Radar Signals in K-Distributed Interference,"Proc.ICEE-96, University of Science and Technology, Tehran– Iran, May 1996.

26- F. Hendessi, M. R. Aref, T. A. Gulliver and A. U. H. Sheikh, "Fast Data Encryption Standard (FDES): A Good Replacement for DES," Proc.18th Biennial Symp. on Communications., Kingstone, Ontario, June 2-5, 1996.

27- M.R. Aref, "the Future of Telecomm. in the Developing Countries in an Era of Changing Policies," Proc. Africa. Telecom, Johannesburg, 1996.

28-Dakhil-Alian, M. R. Aref, "Consideration of Statistical Tests for Stream Cipher Systems," Proc.1st Secure Communication Symposium, Imam Khomeini Univ, March 1997.

29- M. M. Nayebi, M. R. Aref, "The Role of Least Square Estimation in Optimum Detection,"Proc.IEEE-ICT-97, Melbourne, Australia, 2-5 April 1997.

30- Sayadian, M. R. Aref, M. Tabiani, R. Faez, "A New Method for Designing TT-LHSL Reference Patterns for Vector Encoders and Speech Recognition Systems," Proc. ICEE-97, Tehran University, Iran, May 1997.

31- M. M. Nayebi, M. R. Aref, "Limitations of the Gaussian Model for Radar Signals," Proc. IEEE-ISIT, Ulm, Germany, Jun29-July4, 1997.

32- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Coherent Detection of Radar Signal in K-Distributed Interference," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

33- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Coherent Detection of Radar Signal in Weibull-Distributed Interference," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

34- Mirjalili, M. R. Aref, M. M. Nayebi, Kahrizi, "Sensitivity Analysis of Designing Conditions in the Efficiency of a Distributed Detection System for Radar Targets," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

35- Berenjkoub, M. R. Aref, Saeedi, "A Key Distribution Protocol based on a One-Way Function," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

36- Dakhil-Alian, M. R. Aref, Modarres-Hashemi, "Linear Complexity Analysis of Random Sequences and Proposing a Statistical Test," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

37- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Optimal Detection of Slow- Fluctuating Target Signals in Non-Gaussian Noise," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

38- Dakhil-Alian, M. R. Aref, "A New Correlation Test," Proc. ICEE-98, Khaje Nasir Toosi University, Tehran, Iran, May 1998.

39- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Coherent Optimal Linear Detector for Radar Detection in Pseudo Gaussian Noise," Proc. IEEE-ICT-98, Proto Carras, Greece, June 21-25, May 1998.

40- M. Taban, M. R. Aref, H. Alavi, M. M. Nayebi, "Coherent Radar Detection of Rapid Fluctuating Targets in Pseudo-Gaussian Clutters" Proc. IEEE-ICT-98, 1998, Proto Carras, Greece, June 21-25, 1998.

41- A. Sheykhi, M. M. Nayebi, M. R. Aref, "Adaptive Radar Detection in Auto-Regressive Interference," Proc. 1998 Interational Symp. on Noise Reduction for Imaging and Comm. Systems, Tokyo, Japan, Nov 10-12, 1998.

42- Dakhil-Alian, M. R. Aref, Sadeghian, "A Statistical Test based on Symbols Combination," Proc. ICEE-99, Tehran, Iran, May 1999.

43- Dakhil-Alian, M. R. Aref, Sadeghian, "Analysis of Generated Sequences via Chaotic Maps," Proc. ICEE-99, Tehran, Iran, May 1999.

44- Dakhil-Alian, M. R. Aref, Sadeghian, "Design and Statistical Evaluation of Chaotic Pseudo-Random Binary Sequences," Proc. ICEE-99, Tehran, Iran, May 1999.

45- Dakhil-Alian, Aref, Sadeghian, "Proposing a Known-Plaintext Attack for Random Chaotic Models," Proc. ICEE-99, Tehran, Iran, May 1999.

46- Berenjkoub, M. R. Aref, Saeedi, "Design of a Centralized Key Distribution Protocol," Proc. ICEE-99, Tehran, Iran, May 1999.

47- Berenjkoub, Aref, Saeedi, "Evaluation of Krypto-Knight Key Distribution Protocols Family," Proc. 4th Iranian Conference on Computer, Tehran, Iran, May 1999.

48- Mirjalili, M. R. Aref, M. M. Nayebi, "Adaptive Team Decision-Making," Proc. 5th Annual Int. CSI Computer Conf., Shahid Beheshti Univ, March 2000.

49- Mirjalili, Aref, Nayebi, "Optimal Design of Multi-Bit Radar Decision Networks," Proc. IEEE Int. Radar Conf., Washington, May 2000.

50- Mirjalili, Aref, Nayebi, " Optimization of Multi-Bit Detection Networks with Emphasis on False Alarm Rate Stabilization," Proc. ICEE-2000, Isfahan, Iran, May 2000.

51- Berenjkoub, Saeedi, M. R. Aref, "Evaluation and Modification of a Centralized Key Distribution Protocol," Proc. ICEE-2000, Isfahan, Iran, May 2000.

52- Mirjalili, M. R. Aref, M. M. Nayebi, "Adaptive Combination of Receiver Outputs in Multi-Bit Detection Networks," ICEE-2000, Isfahan, Iran, May 2000.

53- A. Sheykhi, M. M. Nayebi, M. R. Aref, "Adaptive Detection of Radar Targets in AR Interference," Proc. ICEE-2000, Isfahan, Iran, May 2000.

54- M. Taban, M. R. Aref, "Coherent Linear Detector for Fast-Fluctuating Targets in Gaussian Interference," Proc. ICEE-2000, Isfahan, Iran, May 2000.

55- Mirjalili, M. R. Aref, M. M. Nayebi, "Optimal Decision Threshold in a Multi-Bit Decision Network," Proc. IEEE Int. Symp. on IT , Italy, June 2000.

56- Rouhi, M. R. Aref, Kalantari, "CDMA in Low Earth Orbit Satellites," Proc. 3rd International Symposium on Small Satellites for Earth Observation, IAA 2001, Berlin, 2-6 April 2001.

57- F. Ashtiani, J. A. Salehi, M. R. Aref, "An Algorithm for New Originating Cells Admission Control in Soft-Handoff Regions in CDMA Cellular Networks," Proc. IST, Tehran, Sept.1-3, 2001.

58- F. Ashtiani, J. A. Salehi, M. R. Aref, "A New Soft-Handoff Management Algorithm with Two Decision Boundaries," Proc. IEEE-PIMRC 2001, San Diego, CA, Sept. 2001.

59- Rouhi, M. R. Aref, Kalantari, "The Role of Power Control in CDMA in Low Earth Orbit Satellites," Proc.APC-MCSTA, Beijing, China, 18-21 Sept. 2001.

60- A. Sheykhi, M. M. Nayebi, M. R. Aref, "A Powerful Practical Coherent Adaptive Radar Detector," Proc. CIE Int. Conf. on Radar, Beijing, China, Oct. 2001.

61- F. Ashtiani, J. A. Salehi, M. R. Aref, "An Approximate Upper Bound for Power-Control Exchange Rate in CDMA Cellular Networks," Proc. Int. Symposium on Telecomm. (IST), Isfahan, Iran, Aug. 2003.

62- F. Ashtiani, J. A. Salehi, M. R. Aref, "Analytical Computation of Spatial Traffic Distribution in a Typical Region of Cellular Network by Proposing a General Mobility Mode," Proc. IEEE-ICT 2003, Tahiti, March 2003.

63- A. Kalantari, A. Ahmadinia , S. Valaee, and M. Aref, "IP Flow Classification on MPLS Networks," in Proc. of the 10th Iranian Conf. Elect. Eng., Tabriz, Iran, , May 14-16, 2002.

64- Olamaee, M. R. Aref, Soleimanipour, "Design of Media Access Control (MAC) Protocol for Multi-Media Traffic over DS-CDMA Systems," Proc. ATNAC, Melbourne, Australia, Dec. 8-10, 2003.

65- Olamaee, M. R. Aref, Soleimanipour, "Token Assignment for Collision Free (TACF) MAC Protocol to Allocate Resources in Multi-Media Wireless Network," Proc. ATNAC, Melbourne, Australia, Dec.8-10, 2003.

66- Olamaee, M. R. Aref, Soleimanipour, " A Non-Collision MAC Protocol for Data and Voice Services in Wireless Network," Proc. ATNAC, Melbourne, Australia, Dec.8-10, 2003.

67- A.A. Tadaion, M. Derakhtian, M.M. Nayebi, M.R. Aref, "BPSK Signal detection Using Generalized Linear Model," in 12th Iranian Conference on Electrical Engineering, Mashhad, Iran, May 7-10 2004.

68- M. Movahhedi, A. A. Tadaion, M. R. Aref, "A Novel Approach to Radio Direction Finding and Detecting the Number of Sources Simultaneously: DMSAE Algorithm," Proc. 34th European Microwave Conf., Vol. 2, Amsterdam, Netherlands, Oct. 2004.

69- A. A. Tadaion, M. Derakhtian, M. M. Nayebi, M. R. Aref, "A Novel Approach to Direction Finding Using UMPI Tests," Proc. IEE Waveform, Diversity and Design, 8-10 Nov. 2004.

70- H.Rouhi, M.R. Aref, M.E. Kalantari, "Investigation the Effect of Different SIR Estimation Methods in Closed Loop Power Control on Outage Probability in CDMA," ICMSAO/2005, American Univ. of Sharjeh, Feb. 2005.

71- H. Rouhi, M. Kalantari, M.R. Aref, "Analysis of the Effects of Related Parameters on Capacity of CDMA Systems," 5th IAA Symposium on Small Satellite for Earth Observation, Berlin, Germany, 4-8 April 2005.

72- H.Rouhi, M. Kalantari, M.R. Aref, "Effects of Different Parameters on the Capacity of Cellular CDMA Systems," 6th World Wireless Congress (WWC' 05) San Francisco, USA, 24-27 May 2005.

73- A.A. Tadaion, M. Derakhtian, S. Gazor, M. R. Aref, "Likelihood Ratio Tests for PSK Modulation Classification in Unknown Noise Environment," Proc. IEEE Canadian Conference on Electrical & Computer Engineering, CCECE2005, May 2005, pp. 151-154.

74- A.A. Tadaion, M. Derakhtian, S. Gazor, M. R. Aref, "Activity Detection of a PSK Signal in Unknown White Gaussian Noise: Optimal & Suboptimal Invariant Detectors," Proc. IEEE Workshop on Statistical Signal Processing, SSPO5, Bordeaux, France 17-20 July 2005

75- A. Payandeh, M.R. Aref, "A New Algorithm for Improving the Remote Sensing Data Transmission over the LEO Satellite Channels," Proc. Int. Conf. on Engg Education (ICEE2005), Gliwice, Poland, July 2005.

76- A. Payandeh, M. Ahmadian, M.R. Aref, "A Novel Joint Source-Channel Coding Scheme for Image Transmission over the LEO Satellite Channel," The 2nd Asian Space Conference (ASC2005), Hanoi, Vietnam, 8-11 Nov. 2005.

77- S.H. Hassani, M.R.Aref, "A New (t,n) Multi-Secret Sharing Scheme Based On Linear Algebra," Proc. IEEE-SECRYPT-2006, 7-10 Aug. 2006

78- A.Zibaee Nejad, F. Ashtiani, M.R. Aref, "Intelligent Eavesdropping of Differential Frequency Hopping," Proc. IEEE Wireless and Microwave Conference, Dec. 2006, Clearwater, Florida.

79- A.Zibaee Nejad, F. Ashtiani, M.R. Aref, "On the Design of Multiple Access Differential Frequency Hopping," Proc. IEEE Wireless and Microwave Conference, Dec. 2006, Clearwater, Florida.

80- M. Tayarani, T. Eghlidos, M.R. Aref, "On the Design of One-Way Key Schedule Algorithms for Block Ciphers," Proc. 15th ICEE2007, 15th-17th May 2007, pp200-206.

81 L. Ghabeli, M.R. Aref, "A New Achievable Rate for Relay Networks and The Capacity of A Class of Semi-Deterministic Relay Networks," IEEE-ISIT 2007, Nice, France, June 2007.

82- A. Zibayi Nejad, M. R. Aref, "Differential Frequency Hopping With Variable Frequency Transition Function," IEEE- Sarnoff 2007.

83- A. Payandeh, M. Ahmadian, M.R. Aref, "A Secure Channel Coding Scheme for Efficient Transmission of Remote Sensing Data Over the LEO Satellite Channels," Proc. IEEE ‚RAST' 2007, June 2007, Turkey, 510-514.

84- M. Tayarani, T. Eghlidos, M.R. Aref, "New Key Schedule Prototype with Provable Security," Proc. WEWoRC, 4th-6th July 2007, Bochum, Germany, pp.157- 162.

85- M. Tayarani, T. Eghlidos, M.R. Aref, "Design Criteria for Key Mixture Functions of Block Ciphers," Proc. WEWoRC, 4th-6th July 2007, Bochum, Germany, pp. 163-165.

86- A. Sobhi Afshar, T. Eghlidos, M.R.Aref, "A McEliece-like Symmetric-Key Cryptosystem based on Quasi-Cyclic Low-Density Parity-Check Codes," Proc. WEWoRC, 4th-6th July 2007, Bochum, Germany, pp. 50-54.

87- M. Ehdaie, T. Eghlidos, M.R. Aref, "A New Threshold Audio Secret Sharing Scheme," Proc. WEWoRC, 4th-6th July 2007, Bochum, Germany, pp. 119-123.

88- B. Bahrak & M.R. Aref, "A Novel Impossible Differential Cryptanalysis of AES," Proc. WEWoRC, 4th-6th July 2007, Bochum, Germany, pp. 152-156.

89- M. Ehdaie, T. Eghlidos, M.R. Aref, "Some New Issues on Secret Sharing Schemes," IEEE ICT 2008, June 2008, Saint Petersburg, Russia.

90- L. Ghabeli, M.R. Aref, "A New Achievable Rate For Relay Networks Based on Parallel Relaying," Proc. IEEE-ISIT2008, July 2008, Montreal, Canada, pp. 1328-1332

91- M. H. Yasayee, M.R. Aref, "Generalized Compress-and-Forward Strategy For Relay," Proc. IEEE-ISIT 2008, July 2008, Montreal, Canada, pp. 2683-2687.

92- M. Rezagholipoor, M. Ahmadian, M.R. Aref, "Robust Network Coding Using Information Flow," Proc. WNC3-08 Workshop, Berlin 2008.

93- M. Rezagholipoor, M. Ahmadian, M.R. Aref, "Static Network Codes Using Network Minimal," Proc. IEEE-ICEE 2008 , March 2008, Lahore, Pakistan.

94- B. Bahrak, T. Eghlidos, M.R. Aref, "Impossible Differential Cryptanalysis of Safer++," Proc. International Conference on Security and Management 2008, Las Vegas, USA, July 2008, pp. 10-14.

95- A. Salimi, M.R. Aref, M. Ahmadian, "Achievability Proof for Degraded Multicast Relay Networks," IEEE-WTS 2008, California, USA.

96- M. Ehdaie, T. Eghlidos, M. R. Aref, "A Novel Secret Sharing Scheme from Audio Perspective," Proc. IEEE-IST 2008, August 2008, Tehran, Iran, pp. 13-18.

97- A. H. Salavati, B. H. Khalaj, M. R. Aref, "A Novel Approach for Providing QoS with Network Coding," Proc. IEEE-IST 2008, August 2008, Tehran, Iran, pp. 446-451.

98- H. Firouzi, M. Ehdaie, M. R. Aref, "A New Method for Visual Secret Sharing," Proc. IEEE-IST 2008, August 2008, Tehran, Iran, pp. 619-623.

99- A. R. Sharifi, M. R. Aref, "An Improved Method of Computing Gröbner Bases from Algebraic Cryptanalytic Perspective," Proc. ISCISC2008, Tehran, Iran, Oct. 2008.

100- A. H. Salavati, B. H. Khalaj, P. Crespo, M. R. Aref, "QoS Network Coding," Proc. IEEE-ISITA 2008, Aucland, New Zealand, Dec. 2008, pp. 429-434.

101- A. Hodtani, M. R. Aref, "Capacity of a More General Class of Relay Channels," Proc. IEEE-ISITA 2008, Aucland, New Zealand, Dec. 2008, pp. 1389-1392

102- S. Salimi, M. Salmasizadeh, M. R. Aref, "Generalized secure distributed source coding," Proc. International Workshop on Coding and Cryptography , Ullensvang ,Norway, May 2009.pp.1-12.

103- M. Nilchian, V. Aref, M. R. Aref, "Partial Cognitive Relay Channels," Proc. IEEE Information Theory Workshop on Networking and Information Theory (ITW) 2009, Volos, Greece, June 2009.

104- H. Moradmand, A. Payandeh, M. R. Aref, "Joint Source-Channel Coding using Finite State Integer Arithmetic Code," Proc. 2009 IEEE International Conference on Electro Information Technology , Univ.og Windsor ,Canada, June 2009.pp. 19- 22.

105- R. Khosravi, B. Akhbari, M. Mirmohseni, H. Firouzi, M. R. Aref, "The Capacity Region of the Parallel Partially Cooperative Relay Broadcast Channel with Unmatched Degraded Subchannels," Proc. IEEE International Symposium on Information Theory(ISIT) 2009, Seoul, South Korea, July 2009.

106- R. Khosravi, M. Mirmohseni, B. Akhbari, M. R. Aref, "Cooperative Relay-Broadcast Channels with Causal Channel State Information," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

107- M. Sefidgaran, B. Akhbari, Y. Mohsenzadeh, M. R. Aref, "Reliable Source Transmission Over Relay Networks With Side Information," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

108- B. Akhbari, M. Mirmohseni, M. R. Aref, "Compress-and-Forward Strategy for The Relay Channel With Non-Causal State Information," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

109- M. H. Yasaee & M. R. Aref, "Slepian-Wolf Coding over Cooperative Networks," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

110- R. Khosravi, B. Akhbari, M. Mirmohseni, H. Firouzi, M. R. Aref, "The Capacity Region of the Parallel Partially Cooperative Relay Broadcast Channel with Unmatched Degraded Subchannels," Proc. IEEE International 2009 Symposium on Information Theory, Seoul, South Korea, July 2009.pp. 189- 193.

111- L. Ghabeli & M. R. Aref, "Simultaneous Partial And Backward Decoding Approach for Two-Level Relay Networks," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

112- A. Salimi, M. Mirmohseni, M. R. Aref, "A New Capacity Upper Bound for "Relay-With-Delay" Channels," Proc. IEEE International Symposium on Information Theory (ISIT) 2009, Seoul, South Korea, July 2009.

113- A. Farhadian, M. R. Aref, "Algebraic Cryptanalysis of AES," Proc. ISCISC09, Isfahan, Iran, pp. 81- 84, Oct 2009.

114- M. Mirmohseni, B. Akhbari, M. R. Aref, "Compress-and-Forward Strategy for the Relay Channel with Causal State Information," Proc. IEEE- ITW09, Taormina, Italy, pp. 426- 430, Oct 2009.

115- M. Fatemi, T. Eghlidos, M. r. Aref, "A Multi-Stage Secret Sharing Scheme Using All-or-Nothing Transform Approach," Proc, International Conference on Information and Communications Security (ICICS 2009) , Beijing, China, pp. 449-458, December 2009.

116- S. SalehKalaibar, Leila Ghabeli, M. R. Aref, "An Achievable Rate Region for Broadcast-Relay Networks with Partial Cooperation between Relays," Proc. Australia Communications 2010 Theory Workshop, Canberra, Australia, pp. 7- 12, February 2010.

117- L. Ghabeli, M. R. Aref, "The Asymmetric Gaussian Parallel Relay Network," proc. Australia Communications 2010 Theory Workshop, Canberra, Australia, pp.77-80, February 2010.

118- S. Saleh- Kalaibar, L. Ghabeli, M. R. Aref, "An Achievable Rate Region for a class of Broadcast-Relay Network," Proc. IEEE- ITW 2010, Cairo, Egypt, pp.1- 7, February2010.

119- S. Salimi, M. Salmasizadeh, M. R. Aref, "Secret Key Sharing in a New Source Model: Rate Regions," Proc. 2010 Australia Communications Theory Workshop, Canberra, Australia, pp. 117-122, February 2010.

120- S. Saleh- Kalaibar, L. Ghabeli, M. R. Aref, "On the Capacity Region of Semi-Deterministic Multiple-Access-Relay-Networks," Proc. Australia Communications 2010 Theory Workshop, Canberra, Australia, pp. 54- 58, February 2010.

121- H. Soleimani, A. R. Sharifi, M. R. Aref, "Improved Related-Key Impossible Differential Attacks on 8-Round AES-256," Proc. Int. Zurich Seminar on Communications (IZS), Zurich, swiss, pp. 37- 40, March 2010.

122- H. Soleimani, A. R. Sharifi, M. R. Aref, "Improved Related-Key Boomerang Cryptanalysis of AES-256," Proc. ICISA 2010, Seoul, South Korea, pp. 1- 7, April 2010.

123- F. Farhat, M. R. Pakravan, M. Salmasizadeh, M. R. Aref, "Locally Multipath Adaptive Routing Protocol Resilient to Selfishness and Wormholes," Proc. ISPEC 2010, Seoul, South Korea, April 2010.pp. 187- 200.

124- A. Sharifi, H. Soleimany, M. R. Aref, "9-Round Attack on AES-256 by a 6-round Property," Proc. ICEE 2010, Isfahan, Iran, May 2010.pp.226- 230.

125- F. Samsami Khodadad, F. Ganji, M. R. Aref, "A Practical Approach for Coherent Signal Surveillance and Blind Parameter Assessment in Asynchoronous DS-CDMA Systems in Multipath channel," Proc. ICEE, Isfahan, Iran, May 2010.pp.305- 310.

126- L. Ghabeli, M. R. Aref, "On Achievable Rates for Relay Networks based on Partial Decode-and-Forward," Proc. IEEE- ISIT- 2010, Texas, America,June2010.

127- B. Akhbari, M. Mirmohseni, M. R. Aref, "State-Dependent Relay Channel with Private Messages with Partial Causal and Non-Causal Channel State Information," Proc. IEEE- ISIT-2010, Texas, America, pp.634- 638, June 2010.

128- S. Saleh-Kalaibar, L. Ghabeli, M. R. Aref, "An Outer Bound on the Capacity Region of Broadcast-Relay-Channel," Proc. IEEE- ISIT- 2010, Texas, America, pp.659- 663, June2010.

129- A. Haghi, R. Khosravi, M. R. Aref, F. A. Marvasti, "The Capacity Region of Fading Multiple Access Channels with Cooperative Encoders and Partial CSIT," Proc. IEEE- ISIT- 2010, Texas, America, pp. 485- 489, June 2010.

130- S. SalehKalaibar, M. R. Aref, "On the Capacity Region of the Degraded Z Channel," Proc. IEEE- ITW 2010, Dublin, Ireland, pp.1- 5, Aug 2010.

131- M. Mirmohseni, B. Akhbari, M. R. Aref, "Capacity Regions for Some Classes of Causal Cognitive Interference Channels with Delay," Proc. IEEE- ITW 2010, Dublin, Ireland, pp.1-5, Aug 2010.

132- R. Khosravi, B. Akhbari, M. R. Aref, "Achievable Rate Regions for Dirty Tape Channels and "Joint Writing on Dirty Paper and Dirty Tape," Proc. IEEE- ITW 2010, Dublin, Ireland, pp.1-5, Aug 2010.

133- M. H. Yassaee, M. R. Aref, "Multiple Access Wiretap Channels with Strong Secrecy," Proc. IEEE- ITW 2010, Dublin, Ireland, pp. 1- 5, Aug.2010.

134- Z. Noferesti, N. Rohani, J. Mohajeri, M. R. Aref, "Distinguishing Attack on Bivium," Proc. IEEE- CIT 2010, Bradford, England , pp.1075- 1078, Aug 2010.

135- H. Soleimani, A. Sharif, B. Bahrak, M. R. Aref, "Cryptanalysis of 7-round AES-128," Proc. ISCISC 2010, Tehran, Iran, pp.61-67, Sep 2010.

136- E. Kazemi, B. Fahimnia, T.Eghlidos, M. R. Aref, "Cryptanalysis of Hash Functions Using Coding Theoretic Approach," Proc. ISCISC 2010, Tehran, Iran, pp. 51- 56, Sep 2010.

137- S. Salimi, M. Salmasizadeh, M. R. Aref, "Secret Key Rate Region of Multiple Access Channel Model," Proc. ISITA 2010, Taichung, Taiwan, pp.197- 202, Oct 2010.

138- S. Saleh-Kalaibar, M. R. Aref, "On the Capacity Region of a Class of Z Channels with Cooperation," Proc. ISITA 2010, Taichung, Taiwan, pp. 464- 468, Oct 2010.

139- B. Akhbari, M. Mirmohseni, M. R. Aref, "Achievable Rate Regions for Interference Channel with Two Relay " Proc. ISITA 2010, Taichung, Taiwan, pp.1018- 1023, Oct 2010.

140- R. Khosravi- Farsani, B. Akhbari, M. R. Aref, "The Capacity Region of a Class of Relay-Broadcast Channels and Relay Channels with Three Parallel Unmatched Subchannels," Proc. ISITA 2010, Taichung, Taiwan, pp. 818- 823, Oct 2010.

141- H. Bafghi, S. Salimi, B.Seyfe, M. R. Aref, "Cognitive Interference Channel with Two Confidential Messages," Proc. IEEE-ISITA2010, Taichung, Taiwan, Oct 2010.

142- S. M. Tabatabaei, M. R. Aref, "The Capacity of a Class of Linear Deterministic Relay Networks," Proc. ISITA 2010, Taichung, Taiwan, pp. 720- 725, Oct 2010.

143- S. Daghighi, A. Payandeh. M. R. Payandeh, M. R. Aref, "Adaptive Random Puncturing based Secure Block Turbo Coding," Proc. IST 2010, Tehran, Iran, Dec 2010.

144- N. Rohani, Z. Noferesti, J. Mohajeri, M. R. Aref, "Guess and Determine Attack on Trivium Family," Proc. IEEE-TrstComm, Hong Kong, Dec2010.

145- N. Rohani, Z. Noferesti, J. Mohajeri, M. R. Aref, "Cryptanalysis of Grain," Proc. FTRA 2010, Jeju, South Korea, Dec 2010.

146- N. Rohani, Z. Noferesti, J. Mohajeri, M. R. Aref, "Guess and Determine Attack on Bivium," Proc. FTRA 2010, Jeju, South Korea, Dec 2010.

147- D. Z. Aghaj, F. Farhat, M. R. Pakravan, M. R. Aref, "Risk of Attack Coefficient Effect on Availability of Ad-hoc Networks,"Proc.2nd IEEE CCNC Research Student Workshop, Las Vegas, America, Jan 2011, pp.166- 168

148- D. Z. Aghaj, F. Farhat, M. R. Pakravan, M. R. Aref, "Game-Theoretic Approach to Mitigate Packet Dropping in Wireless Ad-hoc Network," Proc. 2nd IEEE CCNC Research Student Workshop, Las Vegas, America, Jan 2011, pp.163- 165.

149- R. Aghajani, R.Saadat, M. R. Aref, G. Mirjalili, "SER of M- PSK Modulation in Incremental-Selective Decode-and-Forward Cooperative Communications over Rayleigh Fading Channels," proc. IEEE-CACT-2011,Seoul,South Korea,Feb2011, pp.432-437.

150- R. Aghajani, R. Saadat, M. R. Aref, G. Mirjalili, "Power Allocation for Incremental-Selective Decodeand- Forward Cooperative Communications over Rician Fading Channels," proc. IEEE-ICACT-2011,Seoul,South Korea,Feb2011, pp. 730-734.

151- H. Habibi, M. Alaghband, M. R. Aref, "Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard," Proc. WISTP 2011, Heraklion, Kiribati, June 2011, PP. 254- 263.

152- P. Babaheidarian, S. Salimi, M. R. Aref, "A New Secret Key Agreement Scheme in a Four-Terminal Network," Proc. CWIT- 2011, Canada, July, 2011, pp.151- 154.

153- M. Mirmohseni, B. Akhbari, M. R. Aref, "Capacity Bounds for the Three-User CognitiveZ-Interference Channel," Proc. CWIT- 2011, Canada, July, 2011, pp. 34- 37.

154- M. Mirmohseni, B. Akhbari, M. R. Aref, "Strong Interference Conditions forMultiple Access-Cognitive Interference Channel," Proc. CWIT- 2011, Canada, July, 2011, pp. 178- 181.

155- S. Salehkelaibar, M. R. Aref, "On the Transmission of Correlated Sources Over Relay Channels," Proc. IEEE- ISIT 2011, Saint Petersburg, Rassia, July- Aug 2011, pp. 1409- 1413.

156- F. Shirani, M. Emadi, M. Zamani, M. R. Aref, "A New Method for Variable Elimination in Systems," Proc. IEEE- ISIT 2011, Saint Petersburg, Rassia, July- Aug 2011, pp. 1140- 1144.

157- S. Salimi, M. Salmasi zadeh, M. R. Aref, "Key Agreement over Multiple Access Channel Using Feedback Channel," Proc. IEEE- ISIT 2011, Saint Petersburg, Rassia, July- Aug 2011, pp. 1936- 1940.

158- S. Salehkelaibar, M. R. Aref, "The Capacity Region of a Class of 3-Receiver Broadcast Channels With Two Eavesdroppers," Proc. IEEE- ISIT 2011, Saint Petersburg, Rassia, July- Aug 2011, pp. 1031- 1035.

159- M. Alaghband, M. R. Aref, "A Secure Key Management Framework for Heterogeneous Wireless Sensor Networks," Proc. CMS 2011, Ghent, Belgium, Oct 2011. pp.18-31.

160- H. Habibi, M. Alaghband, M. R. Aref, "Attacks on a lightweight mutual authentication protocol under EPC C-1 G-2 standard," Proc. WISTP2011, Heraklion, Croatia, June 2011.

161- M. Habibi, M. R. Aref, D. Ma, "Addressing Flaws in RFID Authentication Protocols," Proc. INDOCRYPT2011, Institute of Mathematical Sciences, India, Dec 2011.

162- M. Zamani. gholami, M. J. Emadi, F. Shirani Chaharsughi, M.R.Aref, "Multiple Access Channel With Correlated Channel States and Cooperating Ecoders," Proc.IEEE ITW 2011, Paraty, Brazil, Oct 2011.

163- M Beheshti, M Bayat, M Gardeshi, M. R. Aref, "Improvement on Q.Xie threshold proxy signature scheme against collusion attack," Proc ICEE2011, pp.2339-2343, Tehran, Iran, May 2011.

164- N. K.Farahani, S. Hamidin, A. Vahid, F. Ashtiyani, M.R.Aref, "Analytical Evaluation of a New MAC Algorithm for Underwater Wireless Sensor Networks," Proc IEEE-ICT-2012, Lobnan, April 2012.

165-.M. Yassaee, M. R. Aref, A. A. Ghohari, "Achievability Proof via Output Statistics of Random Binning," Proc IEEE-ISIT2012, pp. 1049- 1053, America, July 2012.

166- S. Saleh Kalaibar, M. R. Aref, "On the Secrecy Capacity of 3-Receiver Broadcast Channel With Causal States and Conferencing," Proc IEEE-ICT-2012, America, pp. 1172- 1176, July 2012.

167- S. Saleh Kalaibar, M. R. Aref, "On Source Transmission over Some Classes of Relay Channels," Proc IEEE-ICT-2012, America, pp.1952- 1956, July 2012.

168- F. Haddadpour, M. Yassaee, A. A. Ghohari, M. R. Aref, "Coordination via a Relay," Proc IEEE-ICT-2012, America, pp.3058- 3062, July 2012.

169- M. Yassaee, A. A. Ghohari, M.R.Aref, "Channel Simulation via Interactive Communications," Proc IEEE-ICT-2012, America,pp. 3058-3062, July 2012.

170- M. Shafienejad, M. alagheband, M. R. Aref, "A Combinatorial Key Predistribution Scheme for WSNs with group deployment of nodes," Proc ISCISC-2012, Iran, Sep 2012.

171- S. Salimi, m. Skogland, M. Salmasi zadeh,. M. R. Aref, "Pairwise Secret Key Agreement Using the Source Common Randomness," Proc ISWCS'12, French, Aug 2012.

172- M. Ghanizadeh, M. Mirmohseni, B. Seyfe, M. R. Aref, "On the Achievable Rate Region of a New Gaussian Wiretap Channel With Side Information," Proc IEEE-ITW 2012, Switzerland, Sep 2012.

173- F. Poubabai, M. Emadi, M. R. Aref, "'Lattice Coding for Multiple Access Channels with Common Message and Additive Interference," Proc IEEE-ITW 2012, Switzerland, Sep 2012.

174- A. A. Gohari, M. H. yassaee, M. R. Aref, "Secure Channel Simulation," Proc IEEE-ITW 2012, Switzerland, Sep 2012.

175- M. Ehdaie, N. Alexiou, M. Ahmadian, M. R. Aref, P. Papadimitratos, "Key Splitting for Random Key Distribution Schemes," IEEE NPSec, American, Oct. 2012.

176- M. Gohari, M. Majidi, A. Payandeh, M. R. Aref, "Differential Framework Based on the Conditional Linearity Approximation in QUARK Permutation," C4I, Tehran, Nov. 2012.

177- M. Yassaee, a. A. Ghohari, M.R.Aref, "Channel Simulation via Interactive Communications," Proc IEEE-ISIT2012, America, pp. 3058-3062, July 2012.

178- M. H. Yassaee, M. R. Aref, A. Gohari, "A Technique for Deriving One-Shot Achievability Results in Network Information Theory," Int. Symp. on Information Theory (ISIT), pp. 1287-1291, Istanbul- Turkey, 7-12 July 2013.

179- M. H. Yassaee, M. R. Aref, A. Gohari, "Secure Noisy Network Coding," in Iran Workshop on Communication and Information Theory 2013 (IWCIT), Tehran, 8-9 May 2013.

180- M. H. Yassaee, M. R. Aref, A. Gohari, "Non-Asymptotic Output Statistics of Random Binning and Its Applications", IEEE Symposium on Information Theory (ISIT), pp. 1854-1858, Istanbul- Turkey, 7-12 July 2013.

181- S. Salehkalaibar, M. R. Aref, "Joint Source-Channel Coding for Multiple-Access Wiretap Channels," Int. Symp. on Information Theory (ISIT) pp. 369-373, Istanbul- Turkey, 7-12 July 2013.

182- A. Bereyhi, M. Bahrami, M. Mirmohseni, M. R. Aref, "Empirical Coordination in a Triangular Multiterminal Network," Int. Symp. on Information Theory (ISIT), pp. 2149-2153, Istanbul- Turkey, 7-12 July 2013.

183- M. J. Emadi, M. Nasiri Khormuji, M. Skoglund, M. R. Aref, "Multi-layer Gelfand--Pinsker Strategies for the Generalized Multiple-Access Channel," in Iran Workshop on Communication and Information Theory 2013(IWCIT), Tehran, 8-9 May 2013.

184- Z. Shakeri, A. Fazeli Chaghooshi, M. Mirmohseni, M. R. Aref, "Degrees of Freedom in a Three-User Cognitive Interference Channel," in Iran Workshop on Communication and Information Theory 2013 (IWCIT), Tehran, 8-9 May 2013.

185- M. Bahrami, A. Bereyhi, S. Salehkalaibar, M. R. Aref, "Key Agreement Over A State-Dependent 3-Receiver Broadcast Channel," in Iran Workshop on Communication and Information Theory 2013 (IWCIT), Tehran, 8-9 May 2013.

186- S. Ahmadi, Z. Ahmadian, J. Mohajeri, M. R. Aref, "Biclique Cryptanalysis of Piccolo-80 and 128, International ISC Conference on Information Security & Cryptology, Yazd, August 2013.

187- F. Haddadpour, M. H. Yassaee, M. R. Aref, A. Gohari, "When is it possible to simulate a DMC channel from another?" IEEE-ITW2013, pp.587-591, Sevilla, Sept. 2013.

188- Z. Sohrabi-Bonab, M. R. Alagheband, M. R. Aref, "Traceability Analysis of Quadratic Residue-Based," Eleventh Annual Conference on Privacy, Security and Trust (PST), pp. 61-68, Spain, July 2013.

189- M. Nasiraee, B. Akhbari, M. Ahmadian-Attari, M. R. Aref, "On the Reliable Transmission of Correlated Sources Over Two-Relay Network," IEEE-ITW2013, pp. 395-399, IEEE-ITW2013, pp.587-591, Sevilla, Sept. 2013.

190- A. Gholami, M J. Emadi, M. R. Aref, "Analytical Power Allocation for a Full Duplex," in Iran Workshop on Communication and Information Theory 2013 (IWCIT), Tehran, 8-9 May 2013.

191- H. Zivari, B Akhbari, M. Ahmadian, M. R. Aref, "'Compound Multiple Access Channel with Confidential Messages," IEEE ICC2014, 10-14 Jun 2014, Sydney, Australian, 2014.

192- S. Ahmadi, M. Delavar, J. Mohajeri, M. R. Aref, "Security Analysis of CLEFIA-128," ISCISC-2014, Tehrani, Iran, Sep. 2014.

193- S. A. Azimi, Z. Ahmadian, J. Mohajeri, M. R. Aref, " Impossible Differential Cryptanalysis of Piccolo Lightweight Block Cipher," ISCISC-2014, Tehran, Sep., 2014.

194- R. Rezaee, A. Shah Hosseini, M. R. Pakravan, M. R. Aref, "A Jamming Resilient Rendezvous Protocol for Cognitive Radio Ad-Hoc Networks," The Seventh International Symposium on Telecommunication (IST2014), Tehran, August 2014.

195- B. Abdolmaleki, K. Baghery, B. Akhbari, M. R. Aref, “Attacks and Improvements on Two New-Found RFID Authentication Protocols”, IST 2014, No7, 2014, pp. 895-900.

196- S. Asaad, H. R. Amini Khorasgani, T. Eghlidos, M. R. Aref, “Sharing Secret Using Lattice Construction”, IST 2014, No7, 2014, pp. 901-906.

197- K. Keykhosravi, M. Mahzoon, A. Aminzadeh Gohari, M. R. Aref, "'From Source Model to Quantum Key Distillation: An Improved Upper Bound," Iran Workshop on Communication and Information Theory, Tehran, May 2014.

198- Z. Sohrabi-Bonab, M. R. Alagheband, M. R. Aref, "Formal Cryptanalysis of a CRC-Based RFID Authentication Protocol," The 22nd Iranian Conference on Electrical Engineering (ICEE), May 2014.

199- M. J. Emadi, M. Nasiri Khormuji, M. Skoglund, M. R. Aref, "The Generalized MAC with Partial State and Message Cooperation," Iran Workshop on Communication and Information Theory, Tehran, May 2014.

200- N. Afshar, B. Akhbari, M. R. Aref, "Random Coding Bound for E-capacity Region of the Relay Channel with Confidential Messages", 2014 Iran Workshop on Communication and Information Theory (IWCIT), Tehran, May 2014.

201- R. Rabbaninejad, Z. Ahmadian, M. Salmasizadeh, M. R. Aref, "Cube and Dynamic Cube Attacks on SIMON32/64," ISCISC-2014, Tehran, Sep., 2014.

202- K. Baghery, B. Abdolmaleki, B. Akhbari, M. R. Aref, "Privacy Analysis and Improvements of Two Recent RFID Authentication Protocols," ISCISC-2014, Tehran, Sep., 2014.

203- S. Salehkalaibar, M. R. Aref, "An Achievable Scheme for the One-Receiver, Two-Eavesdropper Broadcast Channel," 2014 Iran Workshop on Communication and Information Theory (IWCIT), Tehran, May 2014.

204- Hamidreza Amini Khorasgani, Saba Asaad, Taraneh Eghlidos, Mohammadreza Aref, "A Lattice-Based Threshold Secret Sharing Scheme," ISCISC-2014, Tehran, Sep., 2014.

205- R. Hooshmand, M. Koochak Shooshtari, T. Eghlidos, M. R. Aref, "Reducing the Key Length of McEliece Cryptosystem," ISCISC-2014, Tehran, Sep., 2014.

206- Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, Mohammad Reza Aref, " Untraceable RFID Authentication Protocols for EPC Compliant Tags," 23rd Iranian Conference on Electrical Engineering (ICEE), 2015.

207- Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari and Mohammad Reza Aref, "Cryptanalysis of Two EPC-based RFID Security Schemes", in 12th International ISC Conference on Information Security and Cryptology (ISCISC), Guilan, 2015.

208- Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, Seyed Mohammad Alavi, Mohammad Reza Aref, "Securing Key Exchange and Key Agreement Security Schemes for RFID Passive Tags," 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, Iran, 2016.

209- Milad Rezaee, Mahtab Mirmohseni and Mohammad Reza Aref, "An Online Transmission Policy for Energy Harvesting Systems with Data Traffic Arrival," Iran Workshop on Communication and Information Theory (IWCIT), 3-4 May 2016, Tehran, Iran, 2016.

210- Amir Hossein Hadavi, Narges Kazempour, Mahtab Mirmohseni and Mohammad Reza Aref, "Secrecy Capacity in Large Cooperative Networks in Presence of Eavesdroppers with Unknown Locations," Iran Workshop on Communication and Information Theory (IWCIT), 3-4 May 2016, Tehran, Iran, 2016.

211- Mohammad Hadi, Mohammad Mahdi Mojahedian and Mohammad Reza Aref, "Dynamic Index Coding Gain over a Complete Bi-directional Side Information Graph," Iran Workshop on Communication and Information Theory (IWCIT), 3-4 May 2016, Tehran, Iran, 2016.

212- Seyed Reza Hoseini Najarkolaei, Mohammad Zare Ahangarkolaei, Siavash Ahmadi and Mohammad Reza Aref, “Biclique Cryptanalysis of Twine-128,” ISCISC 2016, Iran, Shahid Beheshti University of Tehran, 7-8 Sept., 2016.

213- Milad Rezaee, Mahtab Mirmohseni and Mohammad Reza Aref, “Energy Harvesting Systems with Continuous Energy and Data Arrivals: the Optimal Offline and a Heuristic Online Algorithms,” ISCISC 2016, Iran, Shahid Beheshti University of Tehran, 7-8 Sept., 2016.

214- Mohammad Zare Ahangarkolaei, Seyed Reza Hoseini Najarkolaei, Siavash Ahmadi, Mohammad Reza Aref, “Zero Correlation Linear Attack on Reduced Round Piccolo-80,” ISCISC2016, Shahid Beheshti University of Tehran, 7-8 Sept., 2016.

215- Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, Mohammad Reza Aref, “Analysis of Xiao et al.’s Authentication Protocol,” 2016 8th International Symposium on Telecommunications (IST2016).

216- Mohammad Mahdi Mojahedian, Amin Gohari, Mohammad Reza Aref, “On the Equivalency of Reliability and Security Metrics for Wireline Networks,” 2017 IEEE international Symposium on Information Theory(ISIT2017), Aachen, Germany, Jun 25-30, 2017

217- Milad Johnny , Mohammad Reza Aref, "Sum Degrees of Freedom for the K-user Interference Channel Using Antenna Switching," 21th International ITG Workshop on Smart Antennas, Berlin, Germany, 15-17 March 2017.

218- Seyed Reza Hoseini Najarkolaei, Siavash Ahmadi, Mohammad Reza Aref, “A New Approach to Key Schedule Designing,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

219- Siavash Ahmadi, and Mohammad Reza Aref, “Modified Fixed Point Attack on Gost2,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

220- Narges Kazempour, Mahtab Mirmohseni, and Mohammad Reza Aref, “New Techniques for Localization Based Information Theoretic Secret Key Agreement,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

221- Amirreza Sarencheh, Maryam Rajabzadeh Asaar, Mahmoud Salmasizadeh, and Mohammad Reza Aref, “An Efficient Cooperative Message Authentication Scheme in Vehicular Ad-hoc Networks,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

222- Aein Rezaei Shahmirzadi, Seyyed Arash Azimi, Mahmoud Salmasizadeh, Javad Mohajeri, and Mohammad Reza Aref, “Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

223- Ali Soleimani, Mahtab Mirmohseni, and Mohammad Reza Aref, “Physical Layer Security in AF and CF Relay Networks with RF-Energy Harvesting,” ISCISC2017, Shiraz University, Shiraz, Iran, 6-7 Sept., 2017.

224- Milad Johnny, and Mohammad Reza Aref, “Sum Degrees of Freedom for the K-user Interference Channel Using Antenna Switching,” WSA 2017, Berlin, Germany, March 15-17, 2017.

225- Mahdi Mahdavi Oliaiy, Mohammad Hassan Ameri, Javad Mohajeri, Mohammad Reza Aref, “A Verifiable Delegated Set Intersection Without Pairing,” 25th Iranian Conference on Electrical Engineering (ICEE2017), K. N. Toosi University of Technology, Tehran, Iran, 2-4 May 2017.

226- Mehdi Mahdavi Oliaiy, Mahshid Delavar, Mohammad Hassan Ameri, Javad Mohajeri, Mohammad Reza Aref, “On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets,” Proceedings of 14th International ISC Conference on Information Security and Cryptology (ISCISC`2017), Shiraz University, Shiraz, 6-7 September 2017.

227- A Sarancheh, M R Asaar, M Salmasizadeh, M R Aref, "RAPP: An Efficient Revocation Scheme with Authentication and Privacy Preserving for Vehicular Ad-hoc Networks, 7th International Conference on Computer and Knowledge Engineering (ICCKE 2017), Ferdowsi University of Mashhad, Mashhad, Iran, October 26-27 2017.

228- AHA Bafghi, M Mirmohseni, MR Aref, "Joint transfer of energy and information in a two-hop relay channel", Iran Workshop on Communication and Information Theory (IWCIT2017), 1-6, 2017/5/3.

229- SM Sedaghat, MH Ameri, J Mohajeri, MR Aref, "An efficient and secure data sharing in Smart Grid: Ciphertext-policy attribute-based signcryption ", Iranian Conference on Electrical Engineering (ICEE2017), 2003-2008, 2017/5/2.

230- S. Karimani, Z. Naghdabadi, T. Eghlidos, and M. R. Aref, “An LWE-based Verifiable Threshold Secret Sharing Scheme”, accepted for CTCrypt 2018, Russia, Suzdal, 2018.

231- J Gholipour, M Mirmohseni, B Seyfe, MR Aref, "State-dependent multiple access relay channel with cooperating transmia provablytters", Iran Workshop on Communication and Information Theory (IWCIT), p.p. 1-6, 2018.

232- Mohammad Mahdi Mojahedian and Mohammad Reza Aref “Independence Number of Graphs: A Quadratic Optimization Approach,” Submitted to ICEE, Dec. 2018.

233- R Sarenche, P Forghani, MH Ameri, MR Aref, M Salmasizadeh, "An Efficient Secure Scheme for Lossy and Lossless Data Aggregation in Smart Grid", 9th International Symposium on Telecommunications (IST), p.p. 528-534, 2018.

234- MM. Mojahedian, S. Beigi, A. Gohari, MH. Yassaee, and MR. Aref, “A Correlation Measure Based on Vector-Valued LP-Norms,” ISIT, Jan. 2019.

235- M Hadi, MM Mojahedian, MR Aref, MR Pakravan, "Time-Sharing Improves Dynamic Index Coding Delay", Iran Workshop on Communication and Information Theory (IWCIT2019), p.p. 1-6, 2019.

236- Mohammad Beheshti-Atashgah, Mohammd Reza Aref, Majid Bayat, Morteza Barari, “ID-based Strong Designated Verifier Signature Scheme and its Applications in Internet of Things”, 27th Iranian Conference on Electrical Engineering (ICEE 2019), 05 August 2019.

237- N Kazempour, M Mirmohseni, MR Aref, "Private authentication: Optimal information theoretic schemes", IEEE Information Theory Workshop (ITW2019), 2019/8/25.

238- M. Abolpour, M. Mirmohseni, and M. R. Aref, “Outage Performance in Secure Cooperative NOMA,” Iran Workshop on Communication and Information Theory (IWCIT2019), p.p. 1-6, 06 June 2019.

239- A. Rahnama, M. Beheshti-Atashghah, T. Eghlidos, and M. R. Aref, “An Ultra-Lightweight RFID Mutual Authentication Protocol”, 16th International ISC Conference on Information Security and Cryptology, 28-29 Aug. 2019.

240- A. Rahnama, M. Beheshti-Atashghah, T. Eghlidos, and M. R. Aref, “A Lightweight Anonymous Authentication Protocol for IoT Wireless Sensor Networks”, 16th International ISC Conference on Information Security and Cryptology, 28-29 Aug. 2019.

241- S R Hoseini Najarkolari, M A Maddah-Ali, M R Aref, "Secure Coded Multi-Party Computation for Massive Matrices with Adversarial Nodes", Thirty-sixth International Conference on Machine Learning (ICML 2019), 15 Jun. 2019.

242- M Chegenizadeh, M Ali, J Mohajeri, MR Aref, "An Anonymous Attribute-based Access Control System Supporting Access Structure Update", 16th International ISC Conference on Information Security and Cryptology, 28-29 Aug. 2019.

243- R Rabaninejad, SM Sedaghat, MA Attari, MR Aref, "An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over Untrusted Cloud", 25th International Computer Conference, Computer Society of Iran (CSICC2020), 2020/1/1.

244- SRH Najarkolaei, MA Maddah-Ali, MR Aref, "Coded secure multi-party computation for massive matrices with adversarial nodes", Iran Workshop on Communication and Information Theory (IWCIT 2020), 2020/5/26.

245- SA Azimi, A Ranea, M Salmasizadeh, J Mohajeri, MR Aref, V Rijmen, "A Bit-Vector Differential Model for the Modular Addition by a Constant", International Conference on the Theory and Application of Cryptology and Information Security, 2020/12/7.

246- MS Masiha, A Gohari, MH Yassaee, MR Aref, Learning under Distribution Mismatch and Model Misspecification, ISIT 2021, acceped, 2021/4/30.

247- N. Kazempour, M. Mirmohseni, M. R. Aref, "Anonymous Mutual Authentication: An Information Theoretic Framework", IWCIT 2021, Acceped, 2021/04/22.

248- O. Mirzamohammadi, A. Aghabagherloo, M. Salmasizadeh, M. R. Aref, “”, Analysis and Improvement of the SPACF Scheme in Vehicular Ad-Hoc Networks (VANETs), ISCISC 2021, Accepted, 2021/08.

مقالات مجلات فارسی:

۱- محمدرضا عارف، سید محمود مدرس هاشمی،"طراحی و ارزیابی رمزکننده‌های پی‌درپی و معرفی یک ساختار جدید"، نشریه دانشکده فنی، شماره ۵۵، دانشگاه تهران، ۱۳۷۴.

۲- محمددخیل علیان، محمدرضا عارف، بابک صادقیان،"اصلاح آزمون خود همبستگی"، مجله علمی تحقیقاتی استقلال.

۳- مهدی برنجکوب، محمدرضا عارف، حسن سعیدی،"توسعه یک پروتکل توزیع کلید دو سویه مبتنی بر تابع لگاریتم گسسته"، مجله علمی و فنی امیرکبیر، دوره ۲۳، شماره ۲

۴- قاسم میرجلیلی، محمدرضا عارف،"طراحی بهینه شبکه‌های آشکارسازی چند بیتی"، فصلنامه دانشور، دانشگاه شاهد، شماره ۹، اسفند ۱۳۸۱.

۵- محمدرضا تابان، محمدرضا عارف،"آزمونی جدید برای آشکارسازی همدوس سیگنال راداری در تداخل شبه‌گوسی(SIRP)،"مجله فنی مهندسی مدرس، شماره ۲۶، سال ۱۳۸۵، صفحات۴۴-۳۱.

۶- محمد بهشتی آتشگاه، محمدرضا عارف، مرتضی براری، "یک طرح امضای مبتنی بر شناسه با تأییدکننده مشخص جدید به همراه کاربرد آن در خانه‌های هوشمند"، مجله علمی-پژوهشی پدافند الکترونیکی و سایبری، شماره ۴، سال ۱۳۹۶، صفحات ۵۵-۶۷.

۷- محمد بهشتی آتشگاه، محمدرضا عارف و مرتضی براری، " مفاهیم و چالشهای امنیتی اینترنت اشیاء نظامی با محوریت مکانیزم MIoT ایالات متحده آمریکا " ، فصلنامه علمی پژوهشی فرماندهی و کنترل – سال دوم، شماره ۳، پاییز ۱۳۹۷.

۸- محمد بهشتی آتشگاه، محمدرضا عارف، مجید بیات و مرتضی براری، "ارائه چارچوب حفظ حریم خصوصی در سلامت الکترونیک"، فصلنامه علمی پژوهشی فرماندهی و کنترل، سال دوم، شماره ۲، تابستان ۱۳۹۷.

۹- مهدی اصفهانی، هادی سلیمانی، محمدرضا عارف،"پیاده سازی عملی حمله نوین کانال جانبی Flush+Reload بر روی AES"، نشریه علمی «علوم و فناوری‌های پدافند نوین»، شماره ۴، زمستان ۱۳۹۸، صفحات ۳۸۳-۳۹۲.

۱۰- محمدرضا عارف، احمد جعفرنژاد و ابوالفضل کیانی بختیاری، "ارائه چارچوب مناسب (شاخص‌های ترکیبی) ارزیابی آمادگی بنگاه‌ها و شهرکهای صنعتی برای پیاده‌سازی مؤلفه‌های بنیادی انقلاب صنعتی چهارم و توسعه سرمایه‌گذاری" فصلنامه علمی پژوهشی دانش سرمایه‌گذاری، سال هشتم، شماره سی و یکم، پاییز ۱۳۹۸، صفحات ۲۳-۴۸.

۱۱- رضا بیات، مهدی صادقی و محمدرضا عارف، "مدل‌سازی شبکه‌های تنظیم ژنی: مدل‌های کلاسیک، اختلال بهینه برای شناسایی شبکه" فصلنامه پردازش علائم و داده ها، شماره ۲، پیاپی ۴۴، ۹۹/۰۶/۲۴، صفحات ۱۰۱-۱۱۲.

۱۲- نرگس کاظم‌پور، مهتاب میرمحسنی و محمدرضا عارف، "توافق کلید امن مبتنی بر مکان‌یابی نسبی بر پایه تئوری اطلاعات"، نشریه علمی «پدافند الکترونیکی و سایبری»، سال ۸ام، شماره ۲، تابستان ۱۳۹۹، صفحات ۳۵-۴۹.

۱۳- محسن رمضان یارندی، علی اصغر بهنام نیا، محمدرضا عارف و محمدرضا خراشادی زاده، "نقش و تأثیر اقتصاد دیجیتال در الگوی راهبردی پیشرفت دانش و فناوری رمز در جمهوری اسلامی ایران"، نشریه امنیت ملی، سال دهم، شماره ۳۵، بهار ۱۳۹۹، صفحات ۳۲۷-۳۵۸.

مقالات فارسی در کنفرانس‌های داخلی:

۱- محمدرضا عارف، سید محمود مدرس هاشمی، "طراحی و ارزیابی رمزکننده‌های پی‌درپی و معرفی یک ساختار جدید"، نشریه دانشکده فنی دانشگاه تهران، دوره ۵۵، شماره ۰، شماره پیاپی ۱۰۰۰۱۶۶، بهار ۱۳۷۴، صفحات ۵۹-۷۱.

۲- پیام امانی، حمید خالوزاده، محمدرضا عارف،"طراحی جعبه جایگزینی(S-box) سیستم رمزنگاری AES با استفاده از نگاشت آشوبی"، چهارمین کنفرانس انجمن رمز ایران، دانشگاه علم و صنعت ایران، ۲۴-۲۶ مهر ۱۳۸۶،صفحات۹۸-۹۱.

۳- علی‌اکبر تدین، درختیان، محمدرضا عارف، مهدی نایبی،"آشکارسازی سیگنال BPSK با استفاده از مدل خطی تعمیم یافته"، دوازدهمین کنفرانس بین‌المللی برق ایران، مشهد، اردیبهشت ۱۳۸۳.

۴- حجت ا... روحی، محمداسماعیل کلانتری، محمدرضا عارف،"بررسی اثر نرخ تنظیم توان و اندازه پله‌های تنظیم توان بر احتمال قطع در سیستم‌های CDMA"، سیزدهمین کنفرانس مهندسی برق ایران، زنجان، اردیبهشت ۱۳۸۴.

۵- مهدی علاقه‌بند، مجید سلیمان‌پور، محمدرضا عارف،"معرفی و تحلیل یک طرح جدید امضاء رمز"، چهارمین کنفرانس انجمن رمز ایران، دانشگاه علم و صنعت ایران، ۲۶-۲۴ مهر ۱۳۸۶، صفحات ۵۱-۴۵.

۶- محمدرضاقلی‌پور، محمود احمدیان، محمدرضا عارف،"بررسی روابط احتمالی گیرنده بهینه در کدهای تصحیح خطای شبکه"، ICEE2008، دانشگاه تربیت مدرس، اردیبهشت ۱۳۸۷.

۷- محمدرضا قلی‌پور، محمود احمدیان، محمدرضا عارف،"روش سریع طراحی کد شبکه مقاوم در برابر از بین رفتن لینک‌های شبکه"، سیزدهمین کنفرانس ملی انجمن رمز ایران، دانشگاه صنعتی شریف، کیش، اسفند ۱۳۸۶.

۸- بهنام بهرک، ترانه اقلیدس، محمدرضا عارف،"حمله تفاضل ناممکن بهبود یافته به الگوریتم رمز Crypton"، پنجمین کنفرانس بین‌المللی انجمن رمز ایران، دانشگاه صنعتی مالک اشتر، مهرماه ۱۳۸۷.

۹- نیما موسوی، محمود سلماسی‌زاده، محمدرضا عارف،"یک طرح جدید برای ایجاد محرمانگی در شبکه براساس کدگذاری شبکه"، پنجمین کنفرانس بین‌المللی انجمن رمز ایران، دانشگاه صنعتی مالک اشتر، مهرماه ۱۳۸۷.

۱۰- محمدصادق دقیقی، علی پاینده، محمدرضا عارف،"سیستم‌های رمز کلید همگانی جدید مبتنی بر تلفیق سیستم‌های رمز Wu-Dawson و McEliece"، پنجمین کنفرانس بین‌المللی انجمن رمز ایران، دانشگاه صنعتی مالک اشتر، مهرماه ۱۳۸۷.

۱۱- محمدصادق دقیقی، علی پاینده، محمدرضا عارف،"آیا با تغییر ساختار کلیدهای همگانی در سیستم رمز Wu- Dawson می‌توان به نیت بیشتری دست یافت؟"، پنجمین کنفرانس بین‌المللی انجمن رمز ایران، دانشگاه صنعتی مالک اشتر، مهر ماه ۱۳۸۷.

۱۲- سعید زاهدی، رضا ابراهیمی، محمد رضا عارف، "رای گیری الکترونیکی و تکنیک‌های افزایش امنیت و قابلیت اعتماد به آن"، کنفرانس ICEE 2012"، ایران، دانشگاه تهران، اردیبهشت ۲۰۱۲.

۱۳- مجید بیات، محمد سبزی نژاد، محمد رضا عارف، "یک پروتکل تبادل کلید مبتنی بر مشخصه"،کنفرانس ISCIS'12"، ایران، دانشگاه تبریز، شهریور ۲۰۱۲.

۱۴- محمد بهشتی آتشگاه، محمود گردشی، محمد رضا عارف، "یک تی ان طرح امضاء وکالتی آستانه با تایید کننده مشخص جدید در مدل استاندارد"، ایران، دانشگاه تبریز، شهریور ۲۰۱۲.

۱۵- معصومه کوچک شوشتری، محمود احمدیان، محمد رضا عارف، "ارائه یک سیستم رمز کلید عمومی مبتنی بر کد"، ایران، دانشگاه تبریز، شهریور ۲۰۱۲.

۱۶- سعید زاهدی, رضا ابراهیمی, محمدرضا عارف, "رای‌گیری الکترونیکی و تکنیک‌های افزایش امنیت و قابلیت اعتماد به آن," کنفرانس ICEE2012, ایران, دانشگاه تهران, اردیبهشت ۲۰۱۲.

۱۷- معصومه کوچک شوشتری, محمود احمدیان عطاری, محمدرضا عارف, "ارائه یک سیستم رمز کلید عمومی مبتنی برکد," کنفرانس ISCISC2012, ایران, دانشگاه تبریز, ۲۰۱۲.

۱۸- مجید بیات, محمد سبزی نژاد, محمدرضا عارف, "یک پروتکل تبادل کلید مبتنی بر مشخصه," کنفرانس ISCISC2012, ایران, دانشگاه تبریز, ۲۰۱۲.

۱۹- آیدا اخبارزاده، علی پاینده، مجید بیات و محمدرضا عارف، "ارائه یک طرح احراز اصالت سبکوزن برای اینترنت اشیاء، "سیزدهمین کنفرانس بین المللی انجمن رمز ایران، دانشگاه شهید بهشتی، تهران، ۱۸-۱۷ شهریورماه ۱۳۹۵.

۲۰- محمد بهشتی آتشگاه، محمدرضا عارف، مرتضی براری، "کاربردی از یک طرح امضای گروهی در رایانش ابری موبایل به منظور حفظ حریم خصوصی کاربر"، نهمین کنفرانس ملی فرماندهی و کنترل ایران، دانشگاه خوارزمی، ۲۴ آذر ماه ۱۳۹۵.

۲۱- محمد بهشتی آتشگاه، مجید بیات، محمدرضا عارف، "یک طرح احراز اصالت جدید با ویژگی حفظ حریم خصوصی کاربر در اینترنت اشیاء"، چهاردهمین کنفرانس بین‌المللی انجمن رمز ایران، دانشگاه شیراز، شیراز، ۱۵-۱۶ شهریور ماه ۱۳۹۶.

۲۲- محمد بهشتی آتشگاه، محمدرضا عارف و مرتضی براری، "بررسی نقش فناوری زنجیره بلوکی در اینترنت اشیاء"، یازدهمین کنفرانس ملی فرماندهی و کنترل ایران (C4I)، ۱۳۹۸.

۲۳- محمد بهشتی آتشگاه، محمدرضا عارف، "حریم خصوصی در اینترنت اشیاء و ابعاد مختلف آن"، دوازدهمین کنفرانس ملی فرماندهی و کنترل ایران (C4I)، آذر ماه ۱۳۹۹.