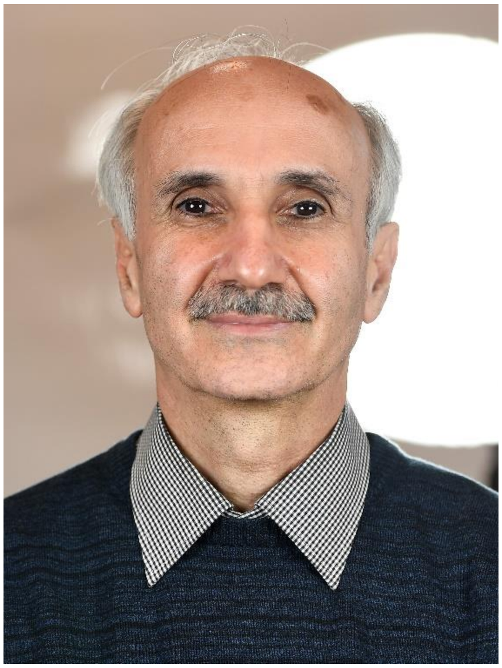
Personal Details:

Name: Javad Mohajeri



Address: P.O. Box: 11155-8639, Electronics Research Institute, Sharif University of Technology, Azadi Ave., Tehran, Iran

Phone number: +98 21 66164961

Fax number: +98 21 66030318

Email: mohajer@sharif.edu, ja.mohajeri@gmail.com

Research Interest:

Analysis and design of Stream Ciphers, Block Ciphers and Public-Key Cryptosystems, and cryptographic protocols such as Electronic voting and Authentication Schemes.

Position:

- Assistant Professor, Electronics Research Institute, Sharif University of Technology, 1990- up to now
- Adjunct assistant professor, Electrical Engineering Department at Sharif University of Technology

- Vice-Chairman in Research, Electronics Research Institute, Sharif University of Technology, 2016-up to now

Experience:

- Part-Time Researcher, Electronics Research Institute, Sharif University of Technology, 1987-1990
- Vice-Chairman in Research, Electronics Research Institute, Sharif University of Technology, 1998-2003
- Founding Member of Iranian Society of Cryptography
- Member of Editorial Board of Biannual Journal for Cyberspace Security MONADI AFTA, 2012-Up to now
- Program Committee member of 2nd, 3rd, 4th, 6th, 7th, 8th, 9th, 10th 11th, 12th, 13th , 14th ,15th and 16th International ISC Conference on Information Security and Cryptology

Instructed Undergraduate Courses:

Calculus (General Math. I, II)

Foundation of Mathematics

Linear Algebra

Discrete Mathematics

Discrete Structures

Graph Theory

Algebra 1 & 2

Introduction to Linear Algebra

Statistics

Instructed Graduated Courses:

Cryptography

Mathematics for Cryptography

Computer & Network Security

Advanced Mathematics

Theses Supervision:

Supervised B.Sc. Theses:

Security Analysis of Public Key Cryptosystems Based on Factorization Problem

Some Supervised M.Sc. Theses:

Design and Cryptanalysis of Clock-Controlled Stream Ciphers

Security Analysis of Threshold Blind Group Digital Signature

Attacks on Smartcards from Leaking Information

Cryptanalysis of Stream Ciphers and Analyzing a Specified Algorithm

Security Analysis of Cell Phones (GSM), Theoretical Principle Collection

Analysis of Stream Ciphers Based on Clock-Controlled Linear Feedback Shift Registers

Maintaining Security in event of Key Exposure

Secure Homomorphic Signature Schemes

Secure Electronic Wallet

Design and Security Analysis of a Computer Network with the Capability of Giving Offline Micro - Payment Service

Comparison of Security Features of 2nd and 3rd Generation of Mobile Systems and Analysis of Authentication and Key Agreement (AKA) Protocol with BAN Logic

Secure Electronic Wallet

Cryptanalysis of Summation Keystream Sequence Generator using Parity Checks with Memory

Power Analysis of DES and AES Block Ciphers Using Power Spectrum Density

Design and improvement of an electronic voting protocol

Improvement and Analysis of Anonymity Methods in Cryptographic Protocols

Distinguish Attack Based on Linear Attacks against Stream Cipher Algorithms

Verification and Analysis of Authentication Protocols

Image Steganography Resistant Against Higher Order Statistical Attacks

Cryptanalysis of a Stream Cipher with Large Variables Using Distinguishing Attack

Modification one of the Boolean Function Generation Method

Distinguishing Attacks on Stream Cipher

Cryptanalysis of Stream Ciphers by Structural Attacks

Cryptanalysis of Verifiable Mix-net

Cryptanalysis of Stream Ciphers Using Statistical Properties of Boolean Functions

Security Improvement of Key Management Protocols in Hierarchical Wireless Sensor Networks

Analysis and Design of RFID Authentication Protocols

Active Distinguishing attack on Stream Ciphers

Security Evaluation of ID-Based Proxy Signature Schemes

Biclique Cryptanalysis of Lightweight Block Ciphers

Cryptanalysis of Lightweight Cryptographic Algorithms

An Untraceable Authentication Protocol

Shortcut Cryptanalysis of Lightweight Block Ciphers

Analysis and Improvement of Id-Based Proxy Signatures

Security Evaluation of Public key based Key Management in MANET

Analysis and Improvement of Secret Handshake Protocols

Biclique Cryptanalysis of Lightweight Block Ciphers

Impossible Differential Cryptanalysis of Lightweight Block Ciphers

Improving the Security of Searchable Encryption Schemes

Design and Security Analysis of Broadcast Authentication Schemes

Attribute Based Keyword Search in Cloud

Improving the Security of Private Set Intersection

Attribute-Based Secure Data Sharing in Smart Grid

Design and Analysis of an E-voting System Based on Blockchain

Analysis and improvement of cryptographic protocols in vehicular ad-hoc networks

Supervised Ph.D. Theses:

Improving attribute-based and searchable cryptographic scheme to provide the security of cloud computing and storage

Keynote Talk: Cryptography: Education, Research, Trends and Organization in Iran and some other countries**,** 10th International ISC Conference on Information Security & Cryptology, 2013

Publication:

Books:

1) J. Mohajeri, A. Farhadian, M. Ahmadian, M. R. Aref, M. Berenjkoob, M. S. Dousti, T. Eghlidos, H. Rostami, M. Salmasizadeh, H. S. Shahhosseini, J. Sheykhzadegan, M. R. Yarandi, "Dictionary and Glossary of Cyberspace Security", Sharif University Press, First Edition,2011
2) J. Mohajeri, A. Farhadian, M. Delavar, M. Ahmadian, M. R. Aref, M. Berenjkoob, M. S. Dousti, T. Eghlidos, H. Rostami, M. Salmasizadeh, H. S. Shahhosseini, J. Sheykhzadegan, M. R. Yarandi, "Dictionary and Glossary of Cyberspace Security", Sharif University Press, Second Edition,2015
3) J. Mohajeri, M. Salmasizadeh, M. Delavar, "Cryptology in Iran and other Countries: Research Challenges, Education, and Administrative Structures", Sharif University Academic Press, 2017

Journal Papers:

1) J. Mohajeri, "Zero-Knowledge Proofs for Independent set and Dominating set Problems", Combinatorics Advances, Kluwer Academic Publishers, pages 251-254, 1995

2) J. Mohajeri, "A Zero-knowledge Proof for Vertex Cover Problem", Scientia Iranica, Volume 6 Number 1, pages 39-43, 1999

3) M. Behdari, M. Salmasizadeh, J. Mohajeri, "Security Architecture of Second Generation of Mobile Communication and its Vulnerabilities", Sharif, Journal of Science & Technology, No. 38, pages 31-41, 2007, (In Persian)

4) K. Azimian, J. Mohajeri, M. Salmasizadeh, "Weak Composite Diffie-Hellman*",* International Journal of Network Security, Vol.7, No.3, PP. 383–387, Nov. 2008.

5) A. Bagherzandi, J. Mohajeri, M. Salmasizadeh, "Comparison based semantic security is probabilistic polynomial time equivalent to indistinguishability ", International Journal of Network Security, Vol.6, No.3, PP.354–360, May 2008

6) M. Rajabzadeh Assar, J. Mohajeri, M. Salmasizadeh, "Another Security Improvement over the Lin et al.'s E-voting Scheme*"* Int. J. Electronic Security and Digital Forensics, Vol. 4, No. 1, PP. 413-422, 2008

7) A. Bagherzandi, J. Mohajeri, M. Salmasizadeh, "A related key Attack on the Feistel type block ciphers", International Journal of Network Security, Vol.8, No.2, PP.219–224, Mar. 2009

8) K. Azimian, J. Mohajeri, M. Salmasizadeh, Samuel S. Wagstaff, " Provable Partial Key Escrow", International Journal of Network Security, Vol.10, No.2, PP.121–124, Mar. 2010.

9) Z. Ahmadian, J. Mohajeri, M. Salmasizadeh, R.M. Hakala, K. Nyberg, “A practical distinguisher for the Shannon Cipher”, Journal of Systems and Software, PP. 543-547, 2010

10) V. Jahandideh, S. A. Mortazavi, Y. Baseri, J. Mohajeri, “Cryptanalysis and security enhancement on the generation of Mu-Varadharajan electronic voting Protocol “, Int. J. Electronic Governance, Vol. 3, No. 1, 2010, PP. 72-84

11) A. Shadman, J. Mohajeri, M. Salmasizadeh, “Linear Distinguishing Attack on a Simplified Version of WG 128”, Sharif Journal of Science & Technology, February-March 2010. (In Persian)

12) Y. Baseri, A. Mortazavi, M. Rajabzadeh Asaar, M. Pourpouneh, J. Mohajeri, “Double Voter Perceptible Blind Signature Based Electronic Voting Protocol”, ISeCure (The ISC International Journal of Information Security), Vol. 3, No.1, PP.43-50, 2011

13) N. Rohani, Z. Noferesti, J. Mohajeri, M. R. Aref, “Guess and Determine Attack on Bivium”, Journal of Information Processing Systems, Vol.7, No.1, March 2011, DOI: 10.3745/JIPS.2011.7.1.151

14) J. Alizadeh, J. Mohajeri, N. Bagheri, “Cryptanalysis of Two Simplified Variants of MD4, Using Linearization”, Journal of Passive Defense Sci. & Tech. 2011, 2, 91-100

15) H. Jannati1, M. Salmasizadeh, J. Mohajeri, A. Moradi, “Introducing proxy zero-knowledge proof and utilization in anonymous credential systems”, SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2012), Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.543

16) A. Vardasbi, M. Salmasizadeh, J. Mohajeri, “On the Multiple Chi-square Test and their Data Complexity”, ISeCure (The ISC International Journal of Information Security), January 2012, Volume 4, Number 1 (pp. 15-24)

17) V. A. Ghaffari, A. Vardasbi, J. Mohajeri, “Cryptanalysis of GSM Encryption Algorithm A5/1”, ISeCure (The ISC International Journal of Information Security), July 2012, Volume 4, Number 2 (pp. 1-8)

18) Y. Baseri, B. Takhataei, J. Mohajeri, “Secure untraceable off-line electronic cash system”, Scientia Iranica, Transactions D - Computer Science & Engineering, 20 (2013) 637–646

19) A. Vardasbi, M. Salmasizadeh, J. Mohajeri, "Superpoly algebraic normal form monomial test on Trivium", IET Information Security, Volume:7, Issue: 3, September 2013, DOI: 10.1049/iet-ifs.2012.0175

20) M. R. Farahani, J. Mohajeri, A. Payandeh, " Impossible Differential Attack on Reduced Round Piccolo-80", Journal of Electronic and Cyber Passive Defense, vol. 2, no. 1, 2014, (In Persian).

21) 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, no. 10, 2014

22) H. A. Yajam, J. Mohajeri, M. Salmasizadeh, "Identity-based universal re-encryption for mixnets ", SECURITY AND COMMUNICATION NETWORKS, Security Comm. Networks (2015), Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1226, 2015

23) M. Delavar, S. Mirzakuchaki, J. Mohajeri, “A Ring Oscillator based PUF (RO-PUF) with Enhanced Challenge-Response Pairs”, Canadian Journal of Electrical and Computer Engineering, Volume 39, Issue 2, DOI:10.1109/CJECE.2016.2521877, 2016

24) M. Delavar, S. Mirzakuchaki, M. H. Ameri, J. Mohajeri, "PUF-based solutions for secure communications in Advanced Metering Infrastructure (AMI)", International Journal of Communication Systems, October 2016, DOI 10.1002/dac.3195

25) A. Mahmoodi, J. Mohajeri, M. Salmasizadeh, "A Certificate-Based Proxy Signature with Message Recovery without Bilinear Pairing", Security and Communication Networks, 2016, DOI: 10.1002/sec.1669

26) S. A. Azimi, S. Ahmadi, Z. Ahmadian, J. Mohajeri, M.R. Aref, "Improved Impossible Differential and Biclique Cryptanalysis of HIGHT", International Journal of Communication Systems, August 2017, DOI: 10.1002/dac.3382, 2017

27) M. Rabaninejad, M. H. Ameri, M. Delavar, J. Mohajeri, “An Attribute-Based Anonymous Broadcast Encryption Scheme with Adaptive Security in the Standard Model”, Scientia Iranica, DOI: 10.24200/SCI.2017.4517, Available Online from 15 October 2017

28) M. H. Ameri, M. Delavar, J. Mohajeri, M. Salmasizadeh, “A Key-Policy Attribute-Based Temporary Keyword Search scheme for Secure Cloud Storage”, IEEE Transactions on Cloud Computing, DOI: 10.1109/TCC.2018.2825983, Date of Publication: 12 April 2018

29) A. R. Shahmirzadi, S. A. Azimi, M. Salmasizadeh, J. Mohajeri, M. R. Aref, “Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher (Extended Version)”, ISeCure (The ISC International Journal of Information Security) January 2018, Volume 10, Number 1 (pp. 3-13)

30) M. Mahdavi Olyaee, M. Delavar, M. H. Ameri, J. Mohajeri, M. R. Aref, “On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets (Extended Version)”,

ISeCure (The ISC International Journal of Information Security) July 2018, Volume 10, Number 2 (pp. 1-11)

31) V. Yousefipoor, M. H., Ameri, J. Mohajeri, T. Eghlidos, "A Secure Attribute-Based Keyword Search Scheme Against Keyword Guessing And Chosen Keyword Attacks", International Journal of Information and Communication Technology (IJICT), Volume 10-Number 1 – Winter 2018 (pp. 48-55)

32) M. H. Ameri, M. Delavar, J. Mohajeri, "Provably Secure and Efficient PUF-based Broadcast Authentication Schemes for Smart Grid Applications", International Journal of Communication Systems, 2019;e3935, DOI: 10.1002/dac.3935

33) S. Ahmadi, Z. Ahmadian, J. Mohajeri, M. R. Aref, "Biclique Cryptanalysis of Block Ciphers LBlock and TWINE-80 with Practical Data Complexity", ISeCure (The ISC International Journal of Information Security), January 2019, Volume 11, Number 1 (pp. 57-73)

34) M. Salmasizadeh, S. A. Mortazavi, J. Mohajeri, "A New Attack on Jakobsson Hybrid Mix-Net", Journal of Electronical & Cyber Defense, Vol. 7, No. 3, 2019, Serial No. 27, (In Persian).

35) M. Ali, J. Mohajeri, M. R. Sadeghi, X. Liu, "A Fully Distributed Hierarchical Attribute-Based Encryption Scheme", Theoretical Computer Science, https://doi.org/10.1016/j.tcs.2020.02.030, 2020

36) M. Ali, J. Mohajeri, M. R. Sadeghi, X. Liu, "Attribute-Based Fine-Grained Access Control for Outscored Private Set Intersection Computation", Information Sciences, Volume 536, October 2020, Pages 222-243, DOI: 10.1016/j.ins.2020.05.041

37) M. M. Modiri, J. Mohajeri, M. Salmasizadeh, "GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication", ISeCure (The ISC International Journal of Information Security), July 2020, Volume 12, Number 2 (pp. 101-111)

38) M.M. Modiri, J. Mohajeri, M. Salmasizadeh, "A Novel Group-based Secure Lightweight Authentication and Key Agreement Protocol for Machine-Type Communication", Accepted Manuscript, Available Online from 23 February 2021 in Scientia Iranica.

Conference Papers:

1) O. Mirzamohammadi, A. Aghabagherloo, J. Mohajeri, M. Salmasizadeh, M.R. Aref, "Analysis and Improvement of the SPACF Scheme in Vehicular Ad-Hoc Networks (VANETs)", 18th International ISC Conference on Information Security & Cryptology, 2021
2) S. Abdollahi, J. Mohajeri, M. Salmasizadeh, "An Efficient and Revocable Fully Outsourced CP-ABE Based on Elliptic Curve Cryptography for IoT", 18th International ISC Conference on Information Security & Cryptology, 2021

3) A. Kavosi, J. Mohajeri, M. Salmasizadeh, (STM'21), "“Efficient Scalable Multi-Party Private Set Intersection Using Oblivious PRF”, The 17th International Workshop on Security and Trust Management, STM2021
4) S. A. Azimi, A. Ranea, M. Salmasizadeh, J. Mohajeri, M. R. Aref, V. Rijmen, “A Bit-Vector Differential Model for the Modular Addition by a Constant”, Asiacrypt 2020
5) M. Doost, A. Kavousi, J. Mohajeri, and M. Salmasizadeh, “Analysis and Improvement of an E-voting System Based on Blockchain”, 28th Iranian Conference on Electrical Engineering (ICEE), 2020
6) A. Kavousi, J. Mohajeri, and M. Salmasizadeh, “Improved Secure Efficient Delegated Private Set Intersection”, 28th Iranian Conference on Electrical Engineering (ICEE), 2020
7) A. Aghabagherloo, J. Mohajeri, and M. Salmasizadeh, “An Efficient Anonymous Authentication Scheme Using Registration List in VANETs”, 28th Iranian Conference on Electrical Engineering (ICEE), 2020
8) M. M. Modiri, J. Mohajeri, M. Salmasizadeh, “GSLHA: Group-based Secure Lightweight Handover Authentication Protocol for M2M Communication”, 16th International ISC Conference on Information Security & Cryptology, 2019 (Selected as the best paper of the conference), DOI: 10.1109/ISCISC48546.2019.8985145
9) M. Cheginizadeh, M. Ali, J. Mohajeri, M. R. Aref, “An Anonymous Attribute-based Access Control System Supporting Access Structure Update, 16th International ISC Conference on Information Security & Cryptology, 2019, DOI: 10.1109/ISCISC48546.2019.8985155
10) A. Aghabagherloo, J. Mohajeri, M. Salmasizadeh, “, On the security of CPPA scheme for intelligent transportation networks”, 16th International ISC Conference on Information Security & Cryptology, 2019
11) M. M. Modiri, J. Mohajeri, M. Salmasizadeh, “GSL-AKA: Group-based Secure Lightweight Authentication and Key Agreement Protocol for M2M Communication”, 9th International Telecommunication Symposium (IST2018), 2018
12) J. Aliakbari, M. Delavar, J. Mohajeri, M. Salmasizadeh, "A Technique to Improve De-anonymization Attacks on Graph Data", 26th Iranian Conference on Electrical Engineering (ICEE2018), DOI: 10.1109/ICEE.2018.8472520
13) M. Kazemi, M. Delavar, J. Mohajeri, M. Salmasizadeh, On the security of an Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks”, 26th Iranian Conference on Electrical Engineering (ICEE2018), DOI: 10.1109/ICEE.2018.8472484
14) M. Mahdavi Olyaee, M. Delavar, M. H. Ameri, J. Mohajeri, M. R. Aref, “On the Security of O-PSI a Delegated Private Set Intersection on Outsourced Datasets”, 14th International ISC Conference on Information Security & Cryptology, 2017
15) A. R. Shahmirzadi, S. A. Azimi, M. Salmasizadeh, J. Mohajeri, M. R. Aref, “Impossible Differential Cryptanalysis of Reduced-Round Midori64 Block Cipher”, 14th International ISC Conference on Information Security & Cryptology, 2017
16) M. Mahdavi Olyaee, M. H. Ameri, J. Mohajeri, M. R. Aref, "A Verifiable Delegated Set Intersection Without Pairing", 25th Iranian Conference on Electrical Engineering, 2017
17) S. M. Sedaghat, M. H. Ameri, J. Mohajeri, M. R. Aref, " An efficient and secure Data Sharing in Smart Grid: ciphertext-policy Attribute-Based Signcryption", 25th Iranian Conference on Electrical Engineering, 2017

18) V. Yousefipoor, M. H., Ameri, J. Mohajeri, T. Eghlidos, " A Secure Attribute-Based Keyword Search Scheme Against Keyword Guessing Attack", 8th International Symposium on Telecommunications, IST 2016, Sep. 2016

19) M. Rabaninejad, M. H. Ameri, M. Delavar, J. Mohajeri, "On The Security of YRL, An Anonymous Broadcast Encryption Scheme",8th International Symposium on Telecommunications, IST 2016, Sep. 2016

20) S. Aghapour, M. H. Ameri, J. Mohajeri, " A Multi Sender Attribute-Based Broadcast Authentication Scheme", 8th International Symposium on Telecommunications, IST 2016, Sep. 2016

21) V. Yousefipoor, M. H., Ameri, J. Mohajeri, T. Eghlidos, " A New Scheme of Sieving Search Results for Attribute-Based Keyword Search in Cloud", 3th International Conference on Applied Research in Computer and Information Technology", February 2016

22) M. A. Ameri, H. Yajam, J. Mohajeri, M. Salmasizadeh, "Verifiable Identity-Based Mix Network", 23rd Iranian Conference on Electrical Engineering (ICEE2015)

23) S. Ahmadi, Z. Ahmadin, J. Mohajeri, M. R. Aref, "Biclique Cryptanalysis of L Block with Modified Key Schedule", 12th International ISC Conference on Information Security & Cryptology, 2015

24) S. Ahmadi, M Delavar, J. Mohajeri, M. R. Aref, " Security Analysis of CLEFIA-128", 11th International ISC Conference on Information Security & Cryptology, 2014

25) S. A. Azimi, Z. Ahmadian, J. Mohajeri, M. R. Aref, " Impossible Differential Cryptanalysis of Piccolo", 11th International ISC Conference on Information Security & Cryptology, 2014

26) H. Yajam, J. Mohajeri, M. Salmasizadeh, " Backward unlinkable and revocable secret handshake without random oracle", 7th International Symposium on Telecommunications (IST), 2014

27) H. Yajam, J. Mohajeri, M. Salmasizadeh, "Identity Based Universal Re-encryption for Mix net", 10th International ISC Conference on Information Security & Cryptology, 2013

28) H. Yajam, A. Mahmoodi, J. Mohajeri, M. Salmasizadeh, " Security Analysis of An Identity -Based Mix Net", 10th International ISC Conference on Information Security & Cryptology, 2013

29) S. Ahmadi, Z. Ahmadian, J. Mohajeri, M. R. Aref, " Biclique Cryptanalysis of Piccolo-80 and 128", 10th International ISC Conference on Information Security & Cryptology, 2013

30) P. Babaheidarian, M. Delavar, J. Mohajeri, “On the Security of an ECC Based RFID Authentication Protocol”, 9th International ISC Conference on Information Security and Cryptology, September 2012.

31) S. Iranian, J. Mohajeri, “Cryptanalysis of Grain-128 Using Active Distinguishing attack”, 9th International ISC Conference on Information Security and Cryptology, September 2012, (In Persian).

32) F. Jamshidi, J. Mohajeri, “A Cluster and Certificateless based Key Management Scheme for Mobile Ad Hoc Networks”, 9th International ISC Conference on Information Security and Cryptology, September 2012, (In Persian).

33) R. Fallah J. Mohajeri, “Server Impersonation Attack on LY, RFID Authentication Protocol”, 17th Annual Computer Society of Iran Computer Conference, 2011. (In Persian).

34) A. Vardasbi, M. Salmasizadeh, J. Mohajeri, “Multiple-Chi-square Tests and Their Application on Distinguishing Attacks”, 8th International ISC Conference on Information Security and Cryptology, 2011.

35) V. Aminghaffari, J. Mohajeri, “An Improved Attack on A5/1”, 8th International ISC Conference on Information Security and Cryptology, 2011.

36) A. Dianat, P. Babaheidarian, J. Mohajeri, “A New Threshold Key Management Scheme for Mobile Ad-Hoc Networks”, 16th Annual Computer Society of Iran Computer Conference, 2010. (In Persian)

37) N. Rohani, Z. Noferesti, J. Mohajeri, M. R. Aref, “Cryptanalysis of Grain”, The 2010 FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA 2010).

38) N Rohani ،Z Noferesti, J. Mohajeri, M.R. Aref, “Guess and Determine Attack on Bivium”, FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA 2010).

39) Z. Noferesti, N. Rohani, J. Mohajeri, M. R., Aref, “Distinguishing Attack on Bivium “10th IEEE International Conference on Computer and Information Technology (CIT 2010) 2010.

40) N Rohani, Z Noferesti, J. Mohajeri, M. R. Aref, “Guess and Determine Attack on Trivium Family”, 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2010.

41) Vardasbi, M. Salmasizadeh, J. Mohajeri,” An Improved Chosen IV Attack on Stream Ciphers”, 7th International ISC Conference on Information Security and Cryptology 2010 (ISCISC’10).

42) R. Samei, J. Mohajeri, “Verification of a Smart Card-Based Remote User Authentication Protocol Using Strand Space Model”, 7th International ISC Conference on Information Security and Cryptology 2010 (ISCISC’10).

43) S. A. Mortazavi, J. Mohajeri, M. Salmasizadeh, “Cryptanalysis of Flash mix-net”, 7th International ISC Conference on Information Security and Cryptology 2010 (ISCISC’10), (In Persian).

44) R. Khani, J. Mohajeri, “New construction of even-variable Boolean functions with maximal algebraic immunity degree based on nonlinearity of function” 15h Annual Computer Society of Iran Computer Conference, 2009, (In Persian).

45) Y. Mohsenzadeh, J. Mohajeri, and S. Ghaemmaghami, “Histogram Shift Steganography: A Technique to Thwart Histogram Based Steganalysis”, Second International Workshop on Computer Science and Engineering, 2009

46) M. Rajabzadeh Assar, J. Mohajeri, M. Salmasizadeh, “Security Modification for the Hwang-Wen-Hwang 's E-voting Scheme”, Proceedings of The 2008 International Conference on Security and Management (SAM’08), Las Vegas, USA, pages 486-490.

47) H. Janati, J. Mohajeri, M. Salmasizadeh, “New Proxy Signature, Proxy Blind Signature, and Blind Proxy Signature Based on Okamoto Signature”, ”, Proceedings of The 2008 International Conference on Security and Management (SAM’08), Las Vegas, USA, pages 238-244.

48) H. Janati, J. Mohajeri, M. Salmasizadeh, “Transferable proxy signature schemes”, Proceedings of 5th International ISC Conference on Information Security & Cryptology 2008, pages 25-35. (In Persian)

49) M. Rajabzadeh Assar, J. Mohajeri, M. Salmasizadeh, “Security Analysis of the Lin et al.'s E-voting Scheme”, Proceedings of 5th International ISC Conference on Information Security & Cryptology 2008, pages 29-33.

50) V. Amin Ghafari, J. Mohajeri, “Linear Distinguish attack on SNOW.2 Using 3 different Masks”,” Proceedings of 5th International ISC Conference on Information Security & Cryptology 2008, pages 96-103. (In Persian)

51) R. Yarandi, J. Mohajeri, A. Mirghadri, “An efficient differential cryptanalysis of Fajr.2 block cipher algorithm” ”, Proceedings of 4th ISC Conference on Information Security & Cryptology 2007, pages 17-24.

52) N. Bagheri, J. Mohajeri, M. Salmasizadeh, “ Differential cryptanalysis Amin.1 block cipher algorithm”, ”, Proceedings of 4th ISC Conference on Information Security & Cryptology 2007, pages 9-16

53) K. Azimian, J. Mohajeri, M. Salmasizadeh, “A New Public Key Encryption Scheme Equivalent to Factoring”, Proceedings of The 2007 International Conference on Security & Management(SAM’07), Las Vegas, USA, pages 552-556.

54) A. Falahati, N. Bagheri, M, Naderi, J, Mohajeri, “ A New Distinguish Attack Against ABC”, Proceedings of the 9th International Conference on Advanced Communication Technology 2007 (ICACT’2007), Korea, pages 1768-1770.

55) E. Jahangiri, J. Mohajeri, “Non-Interactive Publicly Verifiable Partial Key Escrow”, Proceedings of 12th Annual International CSI Computer Conference (CSISS’2005), Tehran, Iran, pages 169-177. (In Persian)

56) K. Azimian, J. Mohajeri, M. Salmasizadeh, “Computing Root Modulo a Composite” Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005). (One of the 8th selected papers), Isfahan, Iran, 2005.

57) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “On the Security of Some Quasigroup Based Encryption Algorithms” Proceedings of IST 2005 (International Symposium on Telecommunications), Shiraz, Iran, 2005.

58) A. Bagherzandi, K. Azimian, J. Mohajeri, M. Salmasizadeh, “Analyzing the relationship between semantic security and indistinguishability against non-adaptive chosen plain text, non-adaptive chosen ciphertext and adaptive ciphertext attacks in a comparing framework” Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005), pages 215-228. (In Persian)

59) M. Amir Mazlaghani, M. Salmasizadeh, J. Mohajeri, “A novel method for exact electronic payment preserving user anonymity” Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005). (In Persian)

60) M. R. Sohizadeh, M. Salmasizadeh, J. Mohajeri, “A novel approach for authentication in networks of compute-constrained devices”, Proceedings of IST 2005 (International Symposium on Telecommunications), Shiraz, Iran, 2005).

61) M. Ramezan Yarandi, A. Mirghadri, J. Mohajeri, ‘‘Efficient Differential Attack upon Fadjr1 Block Cipher Algorithm” Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005). (In Persian)

62) S. Fayyaz Shahandashti, M. Salmasizadeh, J. Mohajeri, “A Provably Secure Short Transitive Signature Scheme from Bilinear Group Pairs”, Proceedings of 4th International Conference, SCN 2004, Amalfi, Italy, Springer Verlag, Lecture Notes in Computer Science, Volume 3352, 2005.

63) M. Salmasizadeh, J. Mohajeri, B. Hajinejad, “Security of Data Exchange in Industrial Control Networks”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 84-96, 2004. (In Persian)

64) S. Mansoori, M. Salmasizadeh, J. Mohajeri, “ Another Vulnerability in Shrinking Generator Stream Cipher ”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 58-65, 2004. (In Persian)

65) K. Azimian, J. Mohajeri, M. Salmasizadeh, “A New Algorithm for Factorization Based on Quadratic Sieve”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 734-742, 2004. (In Persian)

66) M. Salmasizadeh, J. Mohajeri, B. Hajinejad, “Security of Data Exchange in Industrial Control Networks”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 84-96, 2004. (In Persian)

67) S. Mansoori, M. Salmasizadeh, J. Mohajeri, “ Another Vulnerability in Shrinking Generator Stream Cipher ”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 58-65, 2004. (In Persian)

68) K. Azimian, J. Mohajeri, M. Salmasizadeh, “A New Algorithm for Factorization Based on Quadratic Sieve”, Proceedings of 10th Annual Computer Society of Iran Computer Conference, pages 734-742, 2004. (In Persian)

69) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “On the Security of Private keys on Smart Cards under Timing Attack”, Proceedings of IST 2003 (International Symposium on Telecommunications), Isfahan, Iran, 2003.

70) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “Timing Attack on Asymmetric Algorithms Based on Modular Powering” Proceedings of 2nd Iranian Society of Cryptology Conference, pages 58-70, 2003. (In Persian)

71) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “Attack on Classic Implementation of RSA in Smartcards Using Fault Analysis Technique” Proceedings of 2nd Iranian Society of Cryptology Conference, pages 71-79, 2003. (In Persian)

72) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “64-bit Mixer, Araz 64” Proceedings of 2nd Iranian Society of Cryptology Conference, pages 131-141, 2003. (In Persian)

73) H. Boloverdi, J. Mohajeri, M. Salmasizadeh, “Threshold Group Digital Signature”, Proceedings of 8th Annual Computer Society of Iran Computer Conference, pages 31-37, 2003. (In Persian)

74) M. Mohammad Hassanzadeh, J. Mohajeri, M. Salmasizadeh, “ A Novel Attack to Recover Initial State of a Clock-Controlled Cryptosystem with Parameters 1&2”, Proceedings of 7th Annual Computer Society of Iran Computer Conference, pages 1-12, 2002.

75) J. Mohajeri, M. Salmasizadeh, “Cryptanalysis of a Clock Controlled Keystream Generator”, Proceedings of IST 2001 (International Symposium on Telecommunications), Tehran, Iran, pages 468-471, 2001.

76) B. Sadeghian, J. Mohajeri, “Moamegar*:* A 160-bit Block Cipher”, Proceedings of 6th Annual Computer Society of Iran Computer Conference, pages 54-69, 2001.

77) V. Havarinasab, M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “Comparing the First and Last Algorithms in AES Final Selection.”, Proceedings of 1st Iranian Society of Cryptology Conference, pages 253-267, 2001. (In Persian).

78) A. Alavi, B. Mohammadi, A.M. Pezeshk, J. Mohajeri, “Hardware Implementation of RSA and Its Simulation on FPGA ”, Proceedings of 1st Iranian Society of Cryptology Conference, pages 93-104, 2001. (In Persian).

79) M. R. Reyhanitabar, M. Salmasizadeh, J. Mohajeri, “Power Consumption Attack on Smartcard”, Proceedings of 1st Iranian Society of Cryptology Conference, pages 139-149, 2001. (In Persian).

80) M. Mohammad Hassanzadeh, J. Mohajeri, M. Salmasizadeh, “A New Attack on 1 and 2 Clock-Controlled Stream Ciphers”, Proceedings of 1st Iranian Society of Cryptology Conference, pages 151-161, 2001. (In Persian).

81) J. Mohajeri, “A survey on RSA-Like Cryptosystems”, Proceedings of 1st Iranian Society of Cryptology Conference, pages 83-91, 2001. (In Persian).