**Personal Details:**

**Name:** Javad Mohajeri

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

**Phone no.:** +98 21 66164961

**Fax no.:** +98 21 66030318

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

**Educational Records:**

1987-1990, MSC in pure mathematics, Department of Mathematical Science of Sharif University of Technology, Tehran, Iran

1979-1986, BSC in pure mathematics, Department of Science, Isfahan University, Isfahan, Iran

**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

**Experience:**

Part-Time Researcher, Electronics Research Center, Sharif University of Technology, 1987-1990

Full-Time Faculty Member, Electronics Research Institute, Sharif University of Technology, 1990-Up to now

Vice-Chairman in Research, Electronics Research Center, Sharif University of Technology, 1998-2003

Founding Member of Iranian Society of Cryptography

Program Committee member of $2^{nd}$, $3^{rd}$, $4^{th}$, $6^{th}$, $7^{th}$, $8^{th}$, $9^{th}$, $10^{th}$ and $11^{th}$ 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 Liner 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 $2^{nd}$ and $3^{rd}$ Generation of Mobile Systems and Analysis of Authentication and Key Agreement (AKA) Protocol with BAN Logic

Secure Electronic Wallet

Cryptanalysis of Summation Key stream 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

Analyze and Improvement of Secret Handshake Protocols

Biclique Cryptanalysis of Lightweight Block Ciphers

Cryptanalysis of Lightweight Cryptographic Algorithms

An Untraceable Authentication Protocol

Shortcut Cryptanalysis of Lightweight Block Ciphers

**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

**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 OMMUNICATION 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) 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).

20) 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

**Conference Papers:**

1) S. Ahmadi, M Delavar, J. Mohajeri, M. R. Aref, " Security Analysis of CLEFIA-128", 11th International ISC Conference on Information Security & Cryptology, 2014
2) S. A. Azimi, Z. Ahmadian, J. Mohajeri, M. R. Aref, " Impossible Differential Cryptanalysis of Piccolo", 11th International ISC Conference on Information Security & Cryptology, 2014
3) H. Yajam, J. Mohajeri, M. Salmasizadeh, "Identity Based Universal Re-encryption for Mix net", 10th International ISC Conference on Information Security & Cryptology, 2013
4) 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
5) 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
6) 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.
7) 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).
8) 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).
9) R. Fallah J. Mohajeri, "Server Impersonation Attack on LY, RFID Authentication Protocol", 17th Annual Computer Society of Iran Computer Conference, 2011. (In Persian).
10) 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.

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

12) 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)

13) 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).

14) 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).

15) 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.

16) 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.

17) 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).

18) 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).

19) 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).

20) 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).

21) 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

22) 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.

23) 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.

24) 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)

25) 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.

26) 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)

27) 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.

28) 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

29) 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.

30) 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.

31) 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)

32) 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.

33) 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.

34) A. Bagherzandi, K. Azimian, J. Mohajeri, M. Salmasizadeh, "Analyzing the relationship between semantic security and indistinguishablity against none-adaptive chosen plain text,

non-adaptive chosen cipher text and adaptive cipher text attacks in a comparing framework" Proceedings of 3rd Iranian Society of Cryptology Conference (ISCC 2005) , pages 215-228. (In Persian)

35) 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)

36) 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).

37) 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)

38) 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.

39) 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)

40) 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)

41) 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)

42) 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)

43) 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)

44) 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)

45) 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.

46) 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)

47) 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)

48) 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)

49) 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)

50) 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.

51) J. Mohajeri, M. Salmasizadeh, "Cryptanalysis of a Clock Controlled Key stream Generator", Proceedings of IST 2001 (International symposium on Telecommunications), Tehran, Iran, pages 468-471, 2001.

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

53) 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).

54) 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).

55) 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).

56) 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).

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