Berna Örs Yalçın

PERSONAL INFORMATION

Office Address : Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Department of Electronics and Communication Engineering, Maslak, Istanbul, Turkey.
Tel : +90-212-285 36 03
Fax : +90-212-285 35 65
E-mail : siddika.ors@itu.edu.tr
URL : http://web.itu.edu.tr/∼orssi
Birth Date: October 8, 1973
Birth Place: Ankara, TURKEY
Gender: Female
Nationality: Turkish
Marital Status: Married with two children

EDUCATION

Bachelor of Science, Electronics and Communication Engineering
Istanbul Technical University, Faculty of Electrical and Electronics Engineering, June 1995
Graduation Project: Design and Implementation of a Digital Voltmeter
Supervisor: Dr. Kenan İstanbullu

Master of Science, Electronics and Communication Engineering
Istanbul Technical University, Institute of Science and Technology, January 1998
Thesis: Design of Multiplier Blocks for DSP Applications Using VHDL
Supervisor: Prof. Dr. Ahmet Dervişoğlu

Predoctorandus, Electrical Engineering
Katholieke Universiteit Leuven, INSYS Group, June 2000

Ph. D., Applied Science
Katholieke Universiteit Leuven, SCD/COSIC Group, February 2005
Thesis: Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks
Supervisor: Prof. Dr. Bart Preneel, Prof. Dr. Ingrid Verbauwhede

EXPERIENCE

Research and Teaching Assistance 1995 - 2000
Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Department of Electronics and Communication Engineering, Turkey

Research and Teaching Assistance 2000 - 2005
Katholieke Universiteit Leuven, Department of Electrical Engineering, SCD/COSIC Group, Belgium

Assistant Professor 2005 - 2011
Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Department of Electronics and Communication Engineering, Turkey

Head 2007 - Present
Embedded System Design Laboratory, `www.gstl.itu.edu.tr`

- Cryptography
  - Electronic System Design for Cryptography
  - Power consumption / Electromagnetic Propagation Analysis Attacks and Countermeasures
- Modeling and Implementation of Security Protocols
- Embedded System Design and FPGA / ASIC Implementations
  - Secure RFID and Payment Systems
  - Secure Internet of Things Networks (IoT)
  - Digital Signal Processing
  - Image and Video Processing
  - Artificial Neural Networks
  - Deep Learning
  - Random Number Generators
- Application specific processor (ASIP) design and implementation
  - Processor design and implementation
  - Extension and implementation of application-specific instruction set of open source processors

Consultant 2008 - 2009
Embedded Design Center, Eczacibasi Bilisim A.S., Istanbul, Turkey

- Hardware implementations of Advanced Encryption Standard for different performance requirements

Visiting Scholar September 2009 - December 2009
University of California San Diego, Department of Computer Science and Engineering, CA, USA.

- Security of Smart Grid

Associative Professor 2011 - 2020
Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Department of Electronics and Communication Engineering, Turkey

Consultant 2012 - 2014
Anka Microelectronic Systems, Istanbul, Turkey

- SoC Design of LEON 3 Open Source 32-bit Microprocessor, Production as Semiconductor (ASIC) and Implementation of a GPS-based Embedded System Application

Part time Associative Professor 2012 - 2015
Yeditepe University, Faculty of Engineering, Department of Electrical and Electronics Engineering, Turkey

Consultant 2014 - 2017
Defne Telekomunikasyon A.S, Istanbul, Turkey

- Security architecture for smart building systems

Consultant 2015 - 2017
NETA Elektronik A.S, Istanbul, Turkey

- System on Chip Design of a Smart Pay TV Card and Implementation on an FPGA

Consultant 2018 - Present
Güvenpark Bilisim Teknolojileri ArGe Tic. Ltd. Şti, Istanbul, Turkey

- System on Chip (SoC) Design of a Hardware Security Module (HSM) with Zynq Processor, AES, DES, SHA-1, RSA Cryptography Cores and Implementation on an FPGA
- Differential Power and Electromagnetic Analysis Attacks on HSM
- Side-Channel Resistant SoC Design of a HSM with Zynq Processor, AES, DES, SHA-1, SHA-3, RSA, ECC, RNG Cryptography Cores and Implementation on an FPGA
- Side-Channel Resistant SoC Design of a HSM for 5G Standards and Implementation on an FPGA
- Side-Channel Resistant SoC Design of a HSM for Post Quantum Cryptography and Implementation on an FPGA

Professor 2020 - Present
Istanbul Technical University, Faculty of Electrical and Electronics Engineering, Department of Electronics and Communication Engineering, Turkey

COURSES

Bachelor
Basics of Electrical Circuits, Basic Circuit Theory Lab., Circuit and System Analysis, Introduction to Logic Design, Logic Design Laboratory, Digital Systems Design and Applications, Very Large Scale Integrated Circuit Design II
Master

Cryptography, Advanced Digital Design
Ph.D.
Low-power Electronic System Design

SUPERVISED GRADUATION PROJECTS

1. A. Dogan, T. Kaplan, C. Kula, "Hardware Design of Stream Ciphers SFINKS, TRIVIUM, MOSQUITO and Implementation on an FPGA", 2006
2. F. Dayi, "Hardware Design of Stream Cipher A5 Used on GSMs and Implementation on an FPGA", 2006"
3. A. Atici, "Hardware Design of Floating Point Digital IIR Filters and Implementation on an FPGA", 2006
4. V. Celik, "System on Chip Design of Secure Electronic Mail and Implementation on an FPGA", 2008
5. O. Tiryakioglu, "System on Chip Design of Secure Teleconference and Implementation on an FPGA", 2008
6. K. Bulut, "Investigation on Secure Radio Frequency Identification - RFID System and Implementation on a Microprocessor", 2008
7. B. Elci, "Hardware Design of a Steganography System and Implementation on an FPGA", 2008
8. U. Erdogan, "Implementation of Advanced Encryption Standard - AES on a Microprocessor", 2008
9. H.Demirci, Ozgur Yonkuc, "Hardware Design of Hash Functions LANE, Keccak and Implementation on an FPGA", 2009
10. C. Sumengen, "System on Chip Design of Secure Identification Card and Implementation on an FPGA", 2010
11. M. Soybali, "Hardware Design of a Physical Unclonable Function and Implementation on an FPGA", 2010"
12. O. Yelbey, "Hardware Design of Secure Hash Algoritm -SHA and Implementation on an FPGA", 2010
13. M. Oksar, "Hardware/Software Codesign of a Secure Health Care Card and Implementation on an FPGA", 2011
14. S. Ramezani, "Implementation of Computer Arithmetic Algorithms on an FPGA", 2011
15. M. A. Ozkan, "Secure Voice Communication Through GSM Network", 2011
16. S. G. Baskir, "Implementation of a Secure RFID Authentication Algorithm on an FPGA", 2011
17. H. Unlu, "Hardware/Software Codesign of a Distance Bounding Protocol Used in Secure RFID Systems and Implementation on an FPGA", 2011
18. K. Erdogan, "Server Design for Secure RFID System on an Graphical Processing Unit", 2011
19. S. Ozdemir, "Implementation of an Application Using Near Field Communication Technology", 2011

20. I. Demir, “Implementation of a Secure Near Field Communication Application on and FPGA”, 2012
21. M. Usumus, “Implementation of Hash Based Secure RFID Protocol on an FPGA”, 2012
22. O. Sahin, “A Microprocessor Design for Cryptography Applications and Implementation on an FPGA”, 2012
23. S. Alparslan, “Implementation of a Authentication Protocol for Secure RFID Systems Sistemleri”, 2012
24. S. Tuncay, “Implementation of a GSM Modem on an FPGA”, 2012
25. A. Erozan, “Hardware/Software Codesign for Digital Watermarking in DCT Representation Domain”, 2013
26. A. C. Bagbaba, “Implementation of a Secure Near Field Communication System on an FPGA”, 2013
27. G. Kacmaz, “Hardware Design of a Reed-Solomon Decoder and Implementation on an FPGA”, 2013
28. G. Ulutas, “Implementation of a Authentication Protocol for a Secure RFID System”, 2013
29. Y. Gorum, “Implementation of a Secure RFID Protocol Based on Hash Functions on an FPGA”, 2013
30. A. Gencosmanoglu, “A Software-Hardware Implementation Of A Secured Data Communication Protocol Using TEA Algorithm”, 2014
31. A. Jorganxhi, “The Software and Hardware Common Implementation Of A Secure Data Communication Protocol Using AES Algorithm”, 2014
32. B. Bayraktar, “Implementation of a Cryptography Applications Specific Processor on an FPGA”, 2014
33. C. Erdin, “Implementation and Validation of a Secure RFID Protocol”, 2014
34. G. Coktas, “Verification of a Digital System Using Universal Verification Methodology”, 2014
35. M. M. Çetin, “Implementation of Leon3 Processor on an FPGA”, 2014
36. B. Gun,“Design And Implementation Of A Secure Bluetooth Low Energy Communication”, 2015
37. O. Çik, “A Subsystem Design for RFID Tracking System and Implementation on an FPGA”, 2015
38. R. Aktaş, “Distance Estimation Using Received Signal Strength For RFID Tracking System”, 2015
39. O. Azbar, “Hardware/Software Codesign of an RFID Based Indoor Localizatıon System”, 2015
40. A. Oran, “An Indoor Localization Algorithm On FPGA”, 2015
41. O. Bal, “Secure Communication of Microprocessors Using Bluetooth”, 2015 2016
42. E. Yurek, “Writing Drivers For Custom Peripheral Running Parallel To Microblaze Processor on an FPGA”, 2016

43. G. Morgil, “Design and Implementation of an Emergency Evacuation System”, 2016
44. F. Kula, F. Teke, “Design and Verification of An 16-Bit Floating Point ALU, Using Universal Verification Method”, 2017
45. B. Acar, “System on Chip Design of a Lightweight Cryptography Algorithm Boron and Implementation on an FPGA”, 2017
46. C. Bulduk, “Hardware/Software Codesign and Implementation of a Smartcard System”, 2017
47. E. E. Pazarli, “Implementation of Zigbee Protocol on Physical Layer on an FPGA”, 2017
48. O. Sahin, “Implementation of Diffie-Hellman Key Exchange Protocol Using Microblaze on an FPGA”, 2017
49. C. B. Gungor, Y. Ondes, T. T. Sari, B. Uckun, “Instruction Set Extension of Some Processors For Secure IoT Implementations”, 2018
50. B. Ozen, F. Kurt, “Implementation of a Secure Internet of Things Network Using Microprocessors”, 2018
51. Y. Gorur, M. A. Akkaya, “Implementation of Some Lane Tracking Algorithms Using SDSoC and Vivado Platforms on an FPGA”, 2018
52. B. Surer, “Implementation of a SoC By Using LowRISC Processor on an FPGA for Image Filtering Applications”, 2018
53. B. Bilgili, C. Yamaneren, K. Vatansever, U. Çoltu, “System on Chip Design Using Vivado High Level Synthesis Tool”, 2019
54. S. Uslu, M. M. Esen, İ. Guven, “System on Chip Design Using Xilinx Model Composer Tool”, 2019
55. C. Değirmenci, M. Doğan, S. Yavuz, “System on Chip Design of a Visual Cryptography Algrotihm Using Vivado”, 2019
56. M. F. Bagci, “Blink Detection With In-Car Camera on NVIDIA Jetson Tx2 by Neural Network”, 2019
57. M. H. Erdem, Ö. N. Kosebay, E. Sever, “Extension of Instruction Set of Open Source Processors for Specific Applications”, 2019
58. A. Üstün, B. Ateş, M. Antike, “Instruction Set Extension for Post Quantum Cryptography Algorithms on RISC-V Cores”, 2020
59. E. N. İsman, C. Topal, “Extending The Instruction Set of RISC-V Processor for NTRU Algorithm”, 2020
60. M. Kaplan, M. S. Oral, “Power Analysis of FPGA Implementation of DARKRISCV Processor”, 2020
61. A. Eren, M. E. Yagar, “Application-Specific Extension of The Instruction Set of RISC V Processor”, 2020
62. N. A. Koca, B. Yıldız, Y. C. Demirkol, “System on Chip Design for Deep Learning Using Accelerators and Open Source Processor”, 2021
63. F. Can, F. Aydin, F. Gök, “Model Based Design of a Secure Synthetic Radar Signal Processing System Using AES Cryptography Algorithm and Artificial Neural Network”, 2021

64. H. R. Halitoglu, O. Turan, "Model Based Design and Implementation of Secure IoT Network Using Simulink", 2021
65. F. Sala, T. Karakaya, "Model Based Design and Implementation of an IoT Network Resistance Against RPL Routing Attacks", 2021
66. Y. S. Tozlu, Y. Yılmaz, "Design and Implementation Of a 32-Bit RISC-V Core", 2021
67. B. Turgay, "Verification of a Serial Peripheral Interface Intellectual Property By Using Universal Verification Methodology", 2021
68. Ö. Demirci, M. E. Soltekin, "Designing and Implementing Secure Automotive Network for Autonomous Cars", 2021
69. A. Sevgi, M. B. Umutlu, "Implementation of Twin Elevator System Using a PLC", 2022
70. Y. E. Eryılmaz, "Extending the Instruction Set of RISC-V Processor for Ascon Algorithm", 2022
71. A. Turhal, M. Alpaslan, "Custom Direct Memory Access Module Design and Implementation", 2022
72. E. Dinç, G. Baysal, M. Kılıç, "Instruction Extension of RISC-V Processor for Driver Fatigue Detection System and Implementation", 2022
73. S. Daysal, M. E. Tuzcu, "Extending the Instruction Set of RISC-V Processor For Floating-Point Arithmetic", 2022
74. S. Boynueğri, A. F. Yıldız, "Real-Time Filtering of Camera Images With Microblaze Processor", 2022
75. Y. U. Alçalar, S. B. Kapucu, B. Türk, "Realization of Frequency Based Image Steganography Using RISC-V Processor", 2022

SUPERVISED MASTER THESIS

1. N. Mentens, P. Rommens, M. Verhelst, "Timing and Power analysis attacks on the hardware implementation of elliptic curve cryptosystems over $GF(p)$ and $GF\,(2^m)$', *Katholieke Universiteit Leuven, Departement Elektrotechniek - ESAT*, May 2003, Belgium.
2. P. Buysschaert, E. De Mulder, "Electromagnetic analysis attacks on an FPGA implementation of an elliptic curve cryptosystems over $GF(p)$", *Katholieke Universiteit Leuven, Departement Elektrotechniek - ESAT*, May 2004, Belgium.
3. L. Ordu, "Differential Power Analysis Attack Resistant Implementation of the AES Algorithm on an FPGA", 2006
4. H. Kayis, "Differential Power Analysis Attack on an FPGA Implementation of the AES Algorithm", 2006
5. K. Alptekin Bayam, "Power Analysis Resistant Hardware Implementation of The RSA Cryptosystem", 2007
6. I. Yavuz, "An FPGA Implementation of an Elliptic Curve Cryptosystem over $GF\,(3^m))$", 2008
7. F. Karakoc, "Collision Attack on an Microprocessor Implementation of the DES Algorithm", 2008

8. A. Dogan, “Low Power Implementations of the AES Algorithm on an FPGA”, 2008
9. M. Sahinoglu, “Electromagnetic Attacks on FPGA Implementations of the AES Algorithm”, 2008
10. C. Kula, “Differential Power Analysis Attack on an Implementation of the AES Algorithm on a Microporcessor”, 2009
11. T. Kaplan, “Low Power Implementations of the DES Algorithm on an FPGA”, 2009
12. A. Atici, “Low Cost NTRU Implementations”, cosupervisor: Prof. Dr. Ingrid Verbauwhede, 2009
13. U. Kocabas, “Hardware Implementations Of ECC Over A Binary Edwards Curve”, , cosupervisor: Prof. Dr. Ingrid Verbauwhede, 2009
14. D. Bayhan, “Power Efficient FPGA Implementation of RSA Cryptosystem”, 2010
15. Z. Tariguliyev, “Analysis and Characterization of Arbiter PUF”, 2011
16. M. A. Bingol, “Security Analysis of RFID Authentication Protocols Based on Symmetric Cryptography and Implementation of a Forward Private Scheme”, cosupervisor: Gildas Avoine, 2012
17. A. Aris, “Design and Implementation of RSA Cryptosystem Using Partially Interleaved Modular Karatsuba-Ofman Multiplier”, 2012
18. O. Ozkaya, “Analysis of a Location Privacy Preserving RFID Protocol and Implementation on an FPGA”, 2013
19. K. Turksoy, “Differential Power Analysis Attack on an FPGA Implementation of TEA”, 2013
20. A. Ozkan, “Implementation Of a Lightweight Trusted Platform Module”, cosupervisor: Prof. Dr. Ingrid Verbauwhede, 2014
21. S. G. Baskir, “Hardware/Software Codesign and Implementation For Secure Near Field Communication Applications”, 2014
22. A. C. Bagbaba, “Leon3 Microprocessor Based System Design”, 2015
23. L. Akcay, “Implementation and Applications of Open Source OpenRISC Based SOC’s”, 2015
24. B. Ustaoglu, “Fault Tolerant Processor Design”, 2015
25. D. Engin, “Facial Expression Pair Matching”, 2017
26. E. Hatun, “Side Channel Analysis of Implementation of RSA Cryptosystem on Raspberry Pi”, 2018
27. I. Demir, “Fault Injection Attack Resistant Software Design of RSA Cryptosystem on Three Core Leon3 Processor”, 2018
28. U. Esen, “System on Chip Implementation of a New Information Hiding Method”, 2018
29. Y. F. Kula, “Development of Side Channel Analysis Environment Using Simulation Data of System-On-Chip Processors”, 2019
30. M. O. Demirtürk, “Energy Efficient Node Design for Internet Of Things and Implementation on FPGA by Using Open Source Processors and Operating Systems”, 2019

31. A. Seker, “Application Specific Instruction Set Extension of NIOS II Processor”, 2020
32. M. M. Mavi, “Real-Time Sliding Window CLAHE Implementation on FPGA With Variable Clip Limit”, 2020
33. M. Sairoglu, “Low Power General Purpose Processor Design and Instruction Set Extension for AES”, 2020
34. D. Ç. Turunç, “Detection of the Infra-red Pulsed Laser Designation With Infra-red Camera”, 2021
35. E. Gholizadehazari, “An FPGA Implementation of a RISC-V Based SoC System With Custom Instruction Set For Image Processing Applications”, 2021
36. Ö. Altınay, “Instruction Extension Of RV32I and GCC Back End for Ascon Lightweight Cryptography Algorithm”, 2021
37. M. Uzuner, “Model-Based Design and Implementation of Schedulers in Arinc-664 End System as a System On Chip”, 2022
38. T. Keleş, “Model Based Design of Software Define and Cognitive Radio and Implementation on an FPGA”, 2022
39. A. B. Ordu, “Standard Compliant and Authenticated RPL Security Mode Design Against RPL Attacks”, 2022
40. B. Bilgili, “Implementation of 5G Compatible Low Density Parity Check Decoder on FPGA”, cosupervisor: Prof. Dr. Ali Emre Pusane, 2022
41. M. Bayar, “Design of a New Efficient Authentication Method for Wireless Sensor Networks”, 2022
42. M. Ordubağ, “Model-Based Design and Implementation of Target Tracking Filters on an FPGA”, 2022
43. M. Ç. Vuran, “Real Time Dehazing With Dark Channel Prior Method on FPGA”, 2022

PROJECTS

RESEARCHER

2001 - 2005 Identification and Cryptography (G.0141.03), Fonds voor Wetenschappelijk Onderzoek (FWO)

2003 - 2005 Side Channel Analysis Resistant Design Flow (EU IST-2002-507270, SCARD), supported by the European Union

2003 - 2005 European Network of Excellence for Cryptology (EU IST-2002-507932, ECRYPT), supported by the European Union

2010 - 2012 Low-Power Public-Key Cryptography Systems for Smart Cards and Limited Capability Devices, supported by TUBITAK

2011 - 2014 DVB-S/DVB-S2 Demodulator Design and Implementation on an FPGA, Ministry of Industry

2017 - 2020 Design of Reconfigurable Circuits and Systems that can Perform Approximate Computation and their Use in Image Processing Applications Involving Learning, supported by TUBITAK

2021 - 2023 Effective On-Site Clutter Removal and Target Detection with a Low Cost, Mobile Ground Penetrating Radar System, supported by TUBITAK

LEADER

2006 - 2008 Embedded System Design for Cryptographic Algorithms, supported by Istanbul Technical University

2006 - 2008 Side-Channel Attacks Resistant Implementation of AES Algorithm on an FPGA, supported by Istanbul Technical University

2007 - 2010 Side-Channel Resistant Cryptographic System Design and Implementation, supported by TUBITAK

2010 - 2011 Implementation of Gost Standard on a Smartcard, supported by Turkcell

2011 - 2014 Design and Implementation of Secure RFID Systems, supported by TUBITAK

2013 - 2015 Hardware/Software Codesign of Digital Signal Processing Systems, supported by Istanbul Technical University

2018 - 2019 Energy Efficient Sensor Design and Implementation on an FPGA by Using Open Source Processor and Operating Systems, supported by Istanbul Technical University

2018 - 2020 System on Chip Design for Secure IoT Applications, supported by Istanbul Technical University

2020 - 2022 Instruction Extension of RISC-V Processor for Driver Fatigue Detection System and Implementation, supported by TUBITAK

2021 - 2023 Direct Memory Access Module Design and Implementation on an FPGA, supported by TUBITAK

CONSULTANT

2009 – 2010 Advanced Encryption Standard (AES) Hardware Design, Implementation and Integration, supported by TUBITAK

2012 – 2015 SoC Design of LEON 3 Open Source 32-bit Microprocessor, Production as Semiconductor (ASIC) and Implementation of a GPS-based Embedded System Application, supported by TUBITAK

2014 - 2017 Building as a Service (BaaS), supported by European Union

2015 - 2017 Conditional Access Module for Digital Video Broadcast with Common Interface Design and Implementation, supported by TUBITAK

2018 - 2019 National Mobile Whitebox Crypto Library and Peer-to-Peer Communication System Design, supported by TUBITAK

2019 - 2021 High Performance Hardware Security Module Design and Implementation on an FPGA, supported by TUBITAK

2021 - 2022 Hardware Security Module Design for 5G Cryptography Algorithms, supported by TUBITAK

2022 - Hardware Security Module Design for Post Quantum Cryptography Algorithms, supported by TUBITAK

PUBLICATIONS

THESIS

1. B. Örs, "Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks", Ph. D. thesis, Katholieke Universiteit Leuven, February 2005 (ISBN: 90-5682-584-4).
2. B. Örs, "Design of Multiplier Blocks for DSP Applications Using VHDL", M.Sc. Thesis, Istanbul Technical University, February 1999.

EDITED BOOKS

1. B. Örs, B. Preneel, "Cryptography and Information Security in the Balkans", Proceedings of the first International Conference, BalkanCryptSec 2014, Istanbul, Turkey, October 16-17, 2014, Revised Selected Papers, Lecture Notes in Computer Science, Springer, 9024, 2015.
2. B. Örs, "Radio Frequency Identification: Security and Privacy Issues", Proceedings of the 6th International Conference on RFID Security, Lecture Notes in Computer Science, Springer Berlin/Heidelberg, 6370 September 2010.
3. A. Elci, B. Örs, B. Preneel, "Security of Information and Networks", Trafford Publishing, Canada. 2008. ISBN: 978-1-4251-4109-7.

BOOK CHAPTERS

1. B. Örs, B. Preneel, I. Verbauwhede, "Side-Channel Analysis Attacks on Hardware Implementations of Cryptographic Algorithms", Chapter in Wireless Security and Cryptography: Specifications and Implementations, by N. Sklavos (Editor), X. Zhang (Editor), March 30, 2007, CRC Press.
2. B. Örs, F. Gurkaynak, E. Oswald, B. Preneel, "Power-Analysis Attack on an ASIC AES implementation", *Chapter in Embedded Cryptographic Hardware: Design and Security*, Nova Science Publishers, 8 pages, 2004.

JOURNAL PAPERS

1. L. Akcay, B. Örs, "Potential advantages of transport triggered architecture for lattice-based cryptography", the International Journal of Embedded Systems, 2022
2. I. Yavuz, B. Örs, "End-to-End Secure IoT Node Provisioning", Journal of Communications vol. 16, no. 8, pp. 341-346, August 2021, DOI: `https://doi.org/10.12720/jcm.16.8.341-346`

3. L. Akcay, B. Örs, "Comparison of RISC-V and transport triggered architectures for a post-quantum cryptography application", Turkish Journal of Electrical Engineering & Computer Sciences, vol: 29, no: 1, 2021, DOI: https://doi.org/10.3906/elk-2003-27
4. A. Seker, B. Örs, "Instruction Set Extension Of NIOS II for Floating -Point HOG Description and Implementation on an FPGA", Journal of Mechanics of Continua and Mathematical Sciences, Special Issue No. 6, January, 2020, DOI: https://doi.org/10.26782/jmcms.spl.6/2020.01.00003
5. A. Aris, B. Örs Yalcin, S. F. Oktug, "New Lightweight mitigation techniques for RPL version number attacks", Elsevier Ad Hoc Networks, Volume 85, 2019, Pages 81–91, DOI: https://doi.org/10.1016/j.adhoc.2018.10.022
6. S. Gokceli, N. Zhmurov, G. Karabulut Kurt, and B. Örs, "IoT in Action: Design and Implementation of a Building Evacuation Service", Journal of Computer Networks and Communications Volume 2017 (2017), Article ID 8595404, 13 pages DOI: https://doi.org/10.1155/2017/8595404
7. A. Dogan, B. Örs, G. Saldamli, "Analyzing and comparing the AES architectures for their power consumption", Journal of Intelligent Manufacturing, June 2012, Springer, DOI: https://doi.org/10.1007/s10845-012-0671-4
8. Z. Tariguliyev, B. Örs, "Reliability and security of arbiter-based physical unclonable function circuits", International Journal of Communication Systems, Special Issue: Special Issue on Advanced Processing Technologies and Applications for Mobile Communication Systems, Volume 26, Issue 6, pages 757-769, June 2013, John Wiley & Sons, Ltd., DOI: https://doi.org/10.1002/dac.2411
9. G. Avoine, M. A. Bingol, X. Carpent, B. Örs, "Privacy-friendly Authentication in RFID Systems: On Sub-linear Protocols based on Symmetric-key Cryptography", IEEE Transactions on Mobile Computing, Oct. 2013, vol. 12, no. 10, pp. 2037-2049, DOI: https://doi.org/10.1109/TMC.2012.174
10. K. Alptekin Bayam, B. Örs, "Differential Power Analysis Resistant Hardware Implementation of the RSA Cryptosystem", The Turkish Journal of Electrical Engineering & Computer Sciences, Vol.18, No.1, 2010, DOI: https://doi.org/10.3906/elk-0904-4
11. B. Örs, L. Batina, B. Preneel, J. Vandewalle, "Hardware implementation of an Elliptic Curve Processor over GF(p) with Montgomery Modular Multiplier", International Journal of Embedded Systems, Vol. 3, No. 4, 2008, DOI: https://doi/abs/10.1504/IJES.2008.022394
12. E. De Mulder, B. Örs, B. Preneel and I. Verbauwhede, "Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems", An International Journal Computers and Electrical Engineering, 33 (5), p.367-382, Sep 2007, DOI: https://doi.org/10.1016/j.compeleceng.2007.05.009
13. L. Batina, P. Buysschaert, E. De Mulder, N. Mentens, B. Preneel, G. Vandenbosch, I. Verbauwhede, B. Örs, "Side channel attacks and fault attacks on cryptographic algorithms", Revue HF Tijdschrift 2004(4), pp. 36-45, 2004.
14. F. Standaert, B. Örs, B. Preneel J. Quisquater, "Power Analysis Attacks against FPGA Implementations of the DES", *Proceedings of Field-Programmable Logic and*

its Applications (FPL), Lecture Notes in Computer Science, Springer-Verlag, p. 84-94, 2004, DOI: https://doi.org/10.1007/978-3-540-30117-2_11

15. L. Batina, G. Bruin-Muurling, B. Örs, "Flexible Hardware Design for RSA and Elliptic Curve Cryptosystems", *Proceedings of Topics in Cryptology - CT-RSA, The Cryptographers' Track at the RSA Conference*, Tatsuaki Okamoto (Ed.), Lecture Notes in Computer Science 2964, pp. 250-263, San Francisco, CA, USA, February 23-27, 2004, Springer-Verlag, DOI: https://doi.org/10.1007/978-3-540-24660-2_20
16. F. Standaert, B. Örs, B. Preneel, "Power Analysis of an FPGA Implementation of Rijndael: Is Pipelining a DPA Countermeasure?", *Proceedings of Cryptographic Hardware and Embedded Systems - CHES*, Marc Joye, Jean-Jacques Quisquater (Eds.), Lecture Notes in Computer Science (LNCS), Springer-Verlag, pp. 30-44, 2004.
17. N. Mentens, B. Örs, B. Preneel, and J. Vandewalle, "An FPGA Implementation of a Montgomery multiplier over $GF(2^m)$", Computing and Informatics, vol: 23, issue: 5-6, pp. 487-499, 2004.
18. L. Batina, B. Örs, B. Preneel, J. Vandewalle, "Hardware Architectures for Public Key Cryptography", *Elsevier Integration, the VLSI Journal*, issue 34, pages 1-64, 2003, DOI: https://doi.org/10.1016/S0167-9260(02)00053-6
19. B. Örs, Elisabeth Oswald, Bart Preneel, "Power-Analysis Attacks on an FPGA – First Experimental Results", *Proceedings of the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, C. Walter, C. K. Koc and C. Paar (Ed.), 2779 LNCS, pp. 35-50, Cologne, Germany, September 7 - 10 2003, Springer-Verlag.

INTERNATIONAL CONFERENCE PAPERS

1. A. B. Ordu, B. Örs, "RPL Authenticated Mode Evaluation: Authenticated Key Exchange and Network Behavioral", Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), 2022.
2. M. Uzuner, I. Hokelek, B. Örs, "A Model Based Hardware Implementation of Traffic Regulator in ARINC-664 End System", 12th International Conference on Electrical and Electronics Engineering, ELECO 2021.
3. M. Ordubağ, B. Örs, "Model-Based Kalman Filter Design on an FPGA", 12th International Conference on Electrical and Electronics Engineering, ELECO 2021.
4. L. Akçay, B. Örs, "Custom TTA Operations for Accelerating Kyber Algorithm", 12th International Conference on Electrical and Electronics Engineering, ELECO 2021.
5. N. A. Koca, B. Yıldız, Y. C. Demirkol, B. Örs, "Multi-Layer Perceptron Hardware Accelerator on RISC-V Processor", 12th International Conference on Electrical and Electronics Engineering, ELECO 2021.
6. Y. S. Tozlu, Y. Yılmaz, B. Örs, "Design and Implementation Of a 32-Bit RISC-V Core", 12th International Conference on Electrical and Electronics Engineering, ELECO 2021.

7. Ö. Altınay, B. Örs, "Instruction Extension of RV32I and GCC Back End for Ascon Lightweight Cryptography Algorithm", 2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS), DOI: https://doi.org/10.1109/COINS51742.2021.9524190
8. Ö. Özkaya, B. Örs, "System-Level, Model-Based Power Estimation of IoT Nodes", IEEE World Forum on Internet of Things, 14 June-31 July 2021, New Orleans, LA, USA, DOI: https://doi.org/10.1109/WF-IoT51360.2021.9595622
9. C. Topal, E. N. Isman, L. Akcay, B. Örs, "Instruction Extension of an Open Source RV32IMC Core for NTRU Cryptosystem", 24th European Conference on Circuit Theory and Design (ECCTD), September 7-10, 2020, Sofia, Bulgaria.
10. B. Bilgili, C. Yamaneren, K. Vatansever, U. Coltu, B. Örs, "System on Chip Design with Vivado High-Level Synthesis Tool", 11th International Conference on Electrical and Electronics Engineering, ELECO 2019.
11. M. O. Demirtürk, B. Örs , "Low Energy Consuming SoC Design for IoT Applications", 11th International Conference on Electrical and Electronics Engineering, ELECO 2019.
12. E. Hatun, G. Kaya, E. Buyukkaya, B. Örs, "Side Channel Analysis Using EM Radiation of RSA Algorithm Implemented on Raspberry Pi", International Symposium on Networks, Computers and Communications (ISNCC), 2019.
13. S. Buyukcolak, B. Örs, "Simultaneous Image Encryption and Compression Using Modified Huffman Tables", 7th International Conference on Digital Information Processing and Communications (ICDIPC), 2019.
14. F. Kula, B. Örs, "Average Power Consumption Estimation and Momentary Power Consumption Profile Generation of a Softcore Processor", 7th International Conference on Digital Information Processing and Communications (ICDIPC), 2019.
15. L. Akcay, M. Tukel, B. Örs, "Design and implementation of an OpenRISC system-on-chip with an encryption peripheral", European Conference on Circuit Theory and Design, ECCTD 2017.
16. M. Tukel, A. Yurdakul, B. Örs, "A novel template-based multimedia processor array and its toolset", 10th International Conference on Electrical and Electronics Engineering, ELECO 2017.
17. B. Acar, B. Örs, "Hardware/software co-design of a lightweight crypto algorithm BORON on an FPGA", 10th International Conference on Electrical and Electronics Engineering, ELECO 2017.
18. S. Aygun,L. Kouhalvandi, B. Örs, E. O. Gunes, "Karatsuba Ofman Multiplication implementation on SystemC for Diffie-Hellman Key Exchange algorithm", IEEE 4th International Conference on Knowledge-Based Engineering and Innovation, KBEI 2017.
19. S. Gokceli, G. Karabulut Kurt, B. Örs, "Backhaul Infrastructures in Building Automation Systems: Wired or Wireless?", The 3rd IEEE IDAACS Symposium on Wireless Systems within the IEEE International Conferences on Intelligent Data Aquisition and Advanced Computing Systems: Technology and Applications, 26 - 27, September 2016, Offenburg, Germany.

20. B. Ustaoglu, B. Örs, "Fault Tolerant Register File Design for MIPS AES-Crypto Microprocessor", IEEE International Conference on Electronics, Circuits, and Systems (ICECS), Cairo, Egypt, December 06-09, 2015.
21. S. Gokceli, H.B. Tugrel, S. Pisirgen, G. Karabulut Kurt, B. Örs, "A Building Automation System Demonstration", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
22. U. Esen, B. Örs, "Data Hiding Method Using Image Interpolation And Pixel Symmetry", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
23. A.C. Bagbaba, B. Örs, "Hardware Implementation of Novel Image Compression - Encryption System on an FPGA", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
24. O. Azbar, B. Örs, G. Karabulut Kurt, "Implementation of Two Indoor Localization Algorithms on an FPGA", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
25. A.C. Bagbaba, B. Ustaoglu, I. Erdem, B. Örs, "A Layered UVM Based Testbench Design for SpaceWire", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
26. D. Engin, B. Örs, "Implementation of Enigma Machine Using Verilog on an FPGA", 9th International Conference on Electrical and Electronics Engineering (ELECO), 2015.
27. B. Ustaoglu, B. Örs, "Design and implementation of a custom verification environment for fault injection and analysis on an embedded microprocessor", Third International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2015, pages: 256 - 261, DOI: `https://doi.org/10.1109/TAEECE.2015.7113636`
28. A.C. Bagbaba, B. Örs, "Implementation of a secure Near Field Communication system on a FPGA", 8th International Conference on Electrical and Electronics Engineering (ELECO), 2013, DOI: `https://doi.org/10.1109/ELECO.2013.6713921`, pages: 621 - 625.
29. A. Altintas, B. Örs, "System Level Design of Scalable Encryption Algorithm by Using CoWare", The International Conference on Computer, Information, and Telecommunication Systems, CITS 2013.
30. H. Unlu, B. Örs, G. Saldamli, "A New Implementation Methodology for a Secure Distance Bounding Protocol", 7th International Conference on Electrical and Electronics Engineering (ELECO), December 1-4, Bursa, Turkey, 2011.
31. M. A. Ozkan, B. Örs, G. Saldamli, "Secure Voice Communication via GSM Network", 7th International Conference on Electrical and Electronics Engineering (ELECO), December 1-4, Bursa, Turkey, 2011.
32. A. Aris, G. Saldamli, B. Örs, "Architectures for fast modular multiplication", The 14th Euromicro Conference on Digital System Design (DSD) , Oulu, Finland, from August 31st to September 2nd, 2011.

33. M. Oksar, B. Örs, G. Saldamli, "System Level Design of a Secure Healthcare Smart Card System", IEEE Systems and Information Engineering Design Symposium, April 29, 2011, University of Virginia, Charlottesville, VA, USA, 2011.
34. M. Soybali, B. Örs, G. Saldamli, "Implementation of a PUF Circuit on an FPGA", the 4th IFIP International Conference on New Technologies Mobility and Security, 7 - 10 February 2011, Paris, France.
35. D. Bayhan, B. Örs, G. Saldamli, "Analyzing and comparing the Montgomery multiplication algorithms for their power consumption", the 6th IEEE International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 30 November - 2 December, 2010.
36. V. Dalmisli, B. Örs, "Design Of New Tiny Circuits For AES Encryption Algorithm", The 3rd International Conference on Signals, Circuits and Systems (SCS), November 6-8, 2009, Jerba, Tunisia.
37. A. U. Danis, B. Örs, "Differential Power Analysis Attack Considering Decoupling Capacitance Effect", The 19th European Conference on Circuit Theory and Design (ECCTD), August 23-27, 2009, Antalya, Turkey.
38. A. C. Atici, L. Batina, J. Fan, I. Verbauwhede, and B. Örs, "Low-cost Implementations of NTRU for pervasive security", In 19th IEEE International Conference on Application-specific Systems, Architectures and Processors (ASAP), IEEE, pp. 79-84, 2008.
39. I. Yavuz, B. Örs, C. K. Koc, "FPGA Implementation of an Elliptic Curve Cryptosystem over $GF(3^m)$", International Conference on ReConFigurable Computing and FPGAs (ReConFig) , December 3-5, 2008, Cancun, Mexico.
40. K. Alptekin Bayam, B. Örs, "Differential Power Analysis Resistant Hardware Implementation of The RSA Cryptosystem", ISCAS 2008.
41. L. Ordu, B. Örs, "Power Analysis Resistant Hardware Implementations of AES", 14th IEEE International Conference on Electronics Circuits and Systems, December 11-14, 2007.
42. K. Alptekin Bayam, B. Örs, B. Orencik, "A Hardware Implementation of RSA", International Conference on Security of Information and Networks (SIN 2007), May 8-10, 2007, Salamis Bay Conti Resort Hotel, Gazimagusa (TRNC), North Cyprus
43. I. Yavuz, B. Örs, "Hardware Implementation of Elliptic Curve Cryptosystem over $GF(p^m)$", International Conference on Security of Information and Networks (SIN 2007), May 8-10, 2007, Salamis Bay Conti Resort Hotel, Gazimagusa (TRNC), North Cyprus
44. E. De Mulder, B. Örs, B. Preneel and I. Verbauwhede, "Differential Electromagnetic Attack On An FPGA Implementation Of Elliptic Curve Cryptosystems", Proceedings of the World Automation Congress, July 24-26, 2006, Budapest, Hungary.
45. E. De Mulder, P. Buysschaert, B. Örs, P. Delmotte, B. Preneel, G. Vandenbosch and I. Verbauwhede, "Electromagnetic analysis attack on a FPGA implementation of an elliptic curve cryptosystem", Proceedings of the International Conference on Computer as a tool (EUROCON), IEEE, November 21-24, 2005 (Second at IEEE Region 8 Student Paper Contest 2005).

46. L. Batina, J. Lano, N. Mentens, B. Örs, B. Preneel, and I. Verbauwhede, "Energy, Performance, Area versus Security Trade-offs for Stream Ciphers", In ECRYPT Workshop, SASC - The State of the Art of Stream Ciphers, 9 pages, 2004.
47. L. Batina, N. Mentens, B. Örs, B. Preneel, "Serial multiplier architectures over $GF(2^n)$ for elliptic curve cryptosystems", Proceedings of the 12th IEEE Mediterranean Electrotechnical Conference (MELECON), 2004, 12-15 May 2004, Vol.2, pp: 779 - 782.
48. N. Mentens, B. Örs, B. Preneel, J. Vandewalle, "An FPGA Implementation of a Montgomery multiplier over $GF(2^m)$", *Proceedings of the 7th IEEE Workshop on Design & Diagnostics of Electronic Circuits & Systems (DDECS)*, pp. 121-128, 2004.
49. N. Mentens, B. Örs, B. Preneel, "An FPGA Implementation of an Elliptic Curve Processor over $GF(2^m)$", *Proceedings of the 2004 Great Lakes Symposium on VLSI (GLSVLSI 2004)*, pp. 454-457, 2004.
50. B. Örs, F. Gurkaynak, E. Oswald, B. Preneel, "Power-Analysis Attack on an ASIC AES implementation", *Proceedings of the International Conference on Information Technology (ITCC 2004)*, pp. 546-552, 2004.
51. B. Örs, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of an Elliptic Curve Processor over GF(p)", *Proceedings of the IEEE 14th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pp. 433-443, The Hague, The Netherlands, June 24-26, 2003.
52. B. Örs, L. Batina, B. Preneel, J. Vandewalle, "Hardware Implementation of a Montgomery Modular Multiplier in a Systolic Array", *Proceedings of the 10th Reconfigurable Architectures Workshop (RAW)*, 8 pages, Nice, France, April 22, 2003.
53. B. Örs, A. Dervisoglu, "Writing VHDL Models of Parallel nxn Bit Multiplication Blocks", *Proceedings of the European Conferance on Circuit Theory and Design (ECCTD'99)*, pp 402-405, Aug. 1999, Stresa Italy.
54. B. Örs, A. Dervisoglu, "Modeling nxn Multiplication Blocks for DSP Applications Using VHDL", *Proceedings of the 25th EUROMICRO Conference*, pp 892-895, Sept. 8-10 1999, Milan, Italy.

NATIONAL CONFERENCE PAPERS

1. T. Keleş, B. Örs, "Model Based Design of Software Defined and Cognitive Radio and Implementation on an FPGA", 2021 29th Signal Processing and Communications Applications Conference (SIU), DOI: `https://doi.org/10.1109/SIU53274.2021.9477849`
2. E. Gholizadehazari, T. Ayhan, B. Örs, "An FPGA Implementation of a RISC-V Based SoC System for Image Processing Applications", 2021 29th Signal Processing and Communications Applications Conference (SIU), DOI: `https://doi.org/10.1109/SIU53274.2021.9477998`
3. M. O. Demirturk, L. Akcay, B. Örs, "Energy Efficient Sensor Design and Implementation on FPGA by Using Open Source Processors", 27th Signal Processing and Communications Applications Conference (SIU), 2019.

4. O. Ozkaya, B. Örs, "Model based node design methodology for secure IoT applications", 26th Signal Processing and Communications Applications Conference (SIU), 2018, Pages: 1 - 4.
5. A. Arslan, A. C. Bagbaba, B. Sen, B. Örs, "The Walsh-Hadamard transform based automated grading system for monitoring of heart murmurs", National Conference on Electrical, Electronics and Biomedical Engineering, ELECO 2016.
6. L. Akcay, B. Örs, M. Tukel, "Implementation of an OpenRISC Based SoC and Linux Kernel Installation on FPGA", 24th Signal Processing and Communications Applications Conference (SIU), 2016, Pages: 1969 - 1972.
7. B. Ustaoglu, I. Erdem, G. Isik, B. Örs, "Reliability Analysis of MIPS-32 Microprocessor Register Files Designed with Different Fault Tolerant Techniques", 24th Signal Processing and Communications Applications Conference (SIU), 2016.
8. B. Akmansayar, S. Kurtulan, B. Örs, "Design of core blocks and implementation on a programmable logic controller for a train signalization system", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 1942 - 1945, DOI: https://doi.org/10.1109/SIU.2015.7130242
9. H.S. Postalli, S. Tuncay, B. Örs, "Implementation of a modem which transmits digital data on GSM voice channel", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 2537 - 2540, DOI: https://doi.org/10.1109/SIU.2015.7130401
10. B. Ustaoglu, A.C. Bagbaba, B. Örs, I. Erdem, "Creating test environment with UVM for SPI", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 2373 - 2376, DOI: https://doi.org/10.1109/SIU.2015.7130358
11. G. Baskir, B. Örs, "Hardware / software codesign and implementation for secure NFC applications", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 2392 - 2395, DOI: https://doi.org/10.1109/SIU.2015.7130363
12. A.T. Erozan, A.S. Aydogdu, B. Örs, "Application specific processor design for DCT based applications", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 2157 - 2160, DOI: https://doi.org/10.1109/SIU.2015.7130300
13. A.C. Bagbaba, B. Örs, O.S. Kayhan, A.T. Erozan, "JPEG image Encryption via TEA algorithm", 23th Signal Processing and Communications Applications Conference (SIU), 2015, pages: 2090 - 2093, DOI: https://doi.org/10.1109/SIU.2015.7130282
14. A.C. Bagbaba, B. Örs, A.T. Erozan, "Image filtering processor and its applications", 22nd Signal Processing and Communications Applications Conference (SIU), 2014, pages: 2011 - 2014, DOI: https://doi.org/10.1109/SIU.2014.6830653
15. G. Baskir, B. Örs, "Implementation of a secure RFID protocol", 21st Signal Processing and Communications Applications Conference (SIU), 2013, pages: 1 - 4, DOI: https://doi.org/10.1109/SIU.2013.6531442

16. O.E. Ozen, B. Örs, H.B. Yagci, "Design and implementation of a secure RFID system on FPGA", 21st Signal Processing and Communications Applications Conference (SIU), 2013, pages: 1 - 4, DOI: https://doi.org/10.1109/SIU.2013.6531446
17. A.T. Erozan, G. Baskir, B. Örs,"Hardware/Software codesign for watermarking in DCT domain", 21st Signal Processing and Communications Applications Conference (SIU), 2013, pages: 1 - 4, DOI: https://doi.org/10.1109/SIU.2013.6531294
18. S. M. Dilek, B. Örs, M. Kartal, "Reed-solomon decoder hardware implementation for DVB-S receiver", 21st Signal Processing and Communications Applications Conference (SIU), 2013, Pages: 1 - 4, DOI: https://doi.org/10.1109/SIU.2013.6531372
19. Onur Sahin, "Kriptoloji Uygulamalarina Ozel Bir Islemcinin Tasarlanarak FPGA Uzerinde Gerceklenmesi", Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), 29-30 Kasim 2012, Suleyman Demirel Kultur Merkezi, Istanbul Teknik Universitesi, Istanbul
20. S. Tuncay, M. A. Ozkan, B. Örs, "GSM Ses Kanalindan Sayisal Veri Ileten Bir Modemin Tasarimi ve Gerceklenmesi", Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), 29-30 Kasim 2012, Suleyman Demirel Kultur Merkezi, Istanbul Teknik Universitesi, Istanbul
21. S. Alparslan, B. Örs, "Guvenli RFID Sistemleri Icin Bir Kimlik Dogrulama Protokolnun Gerceklenmesi", Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), 29-30 Kasim 2012, Suleyman Demirel Kultur Merkezi, Istanbul Teknik Universitesi, Istanbul
22. B. Elci, S. B. Örs, V. Dalmisli, "Bir Steganografi Sisteminin FPGA Uzerinde Gerceklenmesi", 3. Uluslararasi Katilimli Bilgi Guvenligi ve Kriptoloji Konferansi, 25-27 Aralik 2008, Ankara
23. K. Bulut, S. B. Örs, I. Yavuz, "RFID Sistemlerinin Mikroislemci Uzerinde Guvenli Olacak Sekilde Gerceklenmesi", 3. Uluslararasi Katilimli Bilgi Guvenligi ve Kriptoloji Konferansi, 25-27 Aralik 2008, Ankara
24. V. Dalmisli, S. B. Örs, "Gelismis Sifreleme Standardinin - AES - FPGA Uzerinde Gerceklenmesi", Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, 26-30 Kasim 2008, Bursa
25. V. Celik, S. B. Örs, "Guvenli Elektronik Posta Sistemi PGPnin FPGA Uzerinde Tasarimi Ve Gerceklenmesi", Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, 26-30 Kasim 2008, Bursa
26. L. Ordu, S. B. Örs, "Yan Kanal Analizi Saldirilarina Genel Bakis", Ulusal Elektronik Imza Sempozyumu Bildiriler Kitabi, sayfa: 242-249, 07-08 Aralik 2006

OTHER ACADEMIC ACTIVITIES

- 2020 Security of Information and Networks (SIN), Co-chair
- 2019 Processor Design Workshop - Chair
- 2014 International Conference on Cryptography and Information security - BalkanCryptSec - Chair
- 2010 Radio Frequency Identification: Security and Privacy Issues (RFIDSec), Chair
- 2008 International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), Co-chair

- 2007 Security of Information and Networks (SIN), Co-chair
- 2015, 2016, 2018 International Conference on Cryptography and Information security – BalkanCryptSec, TPC Member
- 2011, 2013, 2015 Radio Frequency Identification: Security and Privacy Issues (RFID-Sec), TPC Member
- 2013 International Conference on Very Large Scale Integration (VLSI-SoC), TPC Member
- 2011, 2013, 2015, 2017 European Conference on Circuit Theory and Design (ECCTD) , TPC Member
- 2014, 2015 2nd International Conference on Electronics and Communication Systems (ICECS) , TPC Member
- 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), TPC Member
- 2012 Workshop on Cryptographic Hardware and Embedded Systems (CHES) , TPC Member

SCOPUS INFORMATION