Prof. Sıddıka Berna Örs Yalçın

Personal Information

Fax Phone: +90 212 285 3565
Email: orssi@itu.edu.tr
Web: http://web.itu.edu.tr/~orssi/
Address: İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Maslak, İstanbul

International Researcher IDs
ORCID: 0000-0003-0851-8501
Publons / Web Of Science ResearcherID: D-8397-2013
ScopusID: 6602685919
Yoksis Researcher ID: 149119

Education Information

Doctorate, Katholieke Universiteit Leuven, Uygulamalı Bilimler, Belgium 1999 - 2005
Postgraduate, Istanbul Technical University, Elektrik-Elektronik Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, Turkey 1995 - 1998
Undergraduate, Istanbul Technical University, Elektrik-Elektronik Mühendisliği Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, Turkey 1991 - 1995

Foreign Languages

English

Dissertations

Doctorate, HARDWARE DESIGN OF ELLIPTIC CURVE CRYPTOSYSTEMS AND SIDE-CHANNEL ATTACKS, Katholieke Universiteit Leuven, Faculteıt Toegepaste Wetenschappen, Departement Elektrotechnıek, 2005
Postgraduate, Design of Multiplier Blocks for DSP Applications Using VHDL, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Ve Haberleşme Mühendisliği Bölümü, 1995

Research Areas

Technical Sciences, Computer Sciences, Information Security and Reliability, Equipment, Electrical and Electronics Engineering, Electronic, Electronic Circuits

Academic Titles / Tasks

Professor, Istanbul Technical University, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2020 - Continues
Associate Professor, Istanbul Technical University, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2011 - 2020
Associate Professor, Bahcesehir University, Faculty Of Engıneerıng, Bilgisayar Mühendisliği, 2017 - 2018

Associate Professor, Yeditepe University, Faculty Of Engıneerıng, Elektrik-Elektronik Mühendisliği, 2012 - 2015
Assistant Professor, Istanbul Technical University, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2005 - 2011
Lecturer PhD, University of California, San Diego, Computer Science And Engineering, 2009 - 2009
Research Assistant, Katholieke Universiteit Leuven, Engineering, Electrical Engineering, 1999 - 2005
Research Assistant, Istanbul Technical University, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 1995 - 2005

Courses

Cryptography, Postgraduate, 2020 - 2021, 2019 - 2020, 2018 - 2019, 2017 - 2018, 2016 - 2017, 2015 - 2016
Circuit and System Analysis, Undergraduate, 2019 - 2020, 2018 - 2019, 2017 - 2018
VLSI Circuit Design II, Undergraduate, 2016 - 2017, 2015 - 2016
Devre ve Sistem Analizi, Undergraduate, 2016 - 2017, 2015 - 2016
Low Power Electronic System Design, Doctorate, 2017 - 2018
Sayısal Sistemler Laboratuvarı, Undergraduate, 2016 - 2017, 2015 - 2016
Sayısal Sistem Tasarımı Uygulamaları, Undergraduate, 2017 - 2018
Cryptography, Postgraduate, 2015 - 2016

Published journal articles indexed by SCI, SSCI, and AHCI

I. **New lightweight mitigation techniques for RPL version number attacks**
Arış A., Yalcin S. B., Oktuğ S. F.
AD HOC NETWORKS, vol.85, pp.81-91, 2019 (SCI-Expanded)

II. **Customizable embedded processor array for multimedia applications**
Tükel M., Yurdakul A., Ors B.
INTEGRATION-THE VLSI JOURNAL, vol.60, pp.213-223, 2018 (SCI-Expanded)

III. **Analyzing and comparing the AES architectures for their power consumption**
DOGAN A., Ors S. B., Saldamli G.
JOURNAL OF INTELLIGENT MANUFACTURING, vol.25, no.2, pp.263-271, 2014 (SCI-Expanded)

IV. **Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography**
AVOINE G., BINGOL M. A., CARPENT X., Yalcin S. B.
IEEE TRANSACTIONS ON MOBILE COMPUTING, vol.12, no.10, pp.2037-2049, 2013 (SCI-Expanded)

V. **Reliability and security of arbiter-based physical unclonable function circuits**
TARIGULIYEV Z., Ors B.
INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, vol.26, no.6, pp.757-769, 2013 (SCI-Expanded)

VI. **Differential power analysis resistant hardware implementation of the RSA cryptosystem**
BAYAM K. A., Ors B.
TURKISH JOURNAL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCES, vol.18, no.1, pp.129-140, 2010 (SCI-Expanded)

VII. **Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems**
DE MULDER E., Oers S. B., Preneel B., VERBAUWHEDE I.
COMPUTERS & ELECTRICAL ENGINEERING, vol.33, pp.367-382, 2007 (SCI-Expanded)

VIII. **Power analysis attacks against FPGA implementations of the DES**
STANDAERT F., Ors S. B., QUISQUATER J., PRENEEL B.
FIELD-PROGRAMMABLE LOGIC AND APPLICATIONS, PROCEEDINGS, vol.3203, pp.84-94, 2004 (SCI-Expanded)

IX. **An FPGA implementation of a Montgomery multiplier over GF(2(M))**

MENTENS N., Ors S. B., PRENEEL B., VANDEWALLE J.
COMPUTING AND INFORMATICS, vol.23, pp.487-499, 2004 (SCI-Expanded)

X. **Power analysis of an FPGA - Implementation of Rijndael: Is pipelining a DPA countermeasure?**
STANDAERT F., Ors S. B., PRENEEL B.
CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2004, PROCEEDINGS, vol.3156, pp.30-44, 2004 (SCI-Expanded)

XI. **Hardware architectures for public key cryptography**
BATINA L., Ors S. B., Preneel B., VANDEWALLE J.
INTEGRATION-THE VLSI JOURNAL, vol.34, pp.1-64, 2003 (SCI-Expanded)

Articles Published in Other Journals

I. **Hardware implementation of an elliptic curve processor over GF(p) with Montgomery modular multiplier**
Örs B., BATINA L., PRENEEL B., VANDEWALLE J.
International Journal of Embedded Systems, vol.3, no.4, pp.229-240, 2008 (Scopus)

II. **Side channel attacks and fault attacks on cryptographic algorithms**
LEJLA B., PETER B., ELKE D. M., NELE M., BART P., VANDENBOSCH G., INGRİD V., ÖRS YALÇIN S. B.
Revue HFTijdschrift, vol.4, pp.36-45, 2004 (Peer-Reviewed Journal)

Refereed Congress / Symposium Publications in Proceedings

I. **System on Chip Design with Vivado High-Level Synthesis Tool**
Bilgili B., Yamaneren C., Vatansever K., Çoltu U., ÖRS YALÇIN S. B.
11th INTERNATIONAL CONFERENCE on ELECTRICAL and ELECTRONICS ENGINEERING, 28 - 30 November 2019

II. **Low Energy Consuming SoC Design for IoT Applications**
Demirtürk M. O., Örs Yalçın S. B.
11th INTERNATIONAL CONFERENCE on ELECTRICAL and ELECTRONICS ENGINEERING, Bursa, Turkey, 28 - 30 November 2019, pp.479-483

III. **Energy Efficient Sensor Design and Implementation on FPGA by Using Open Source Processors**
Demirtürk M., Akçay L., Örs Yalçın S. B.
SİU 2019, Sivas, Turkey, 24 - 26 April 2019, pp.1-4

IV. **Average Power Consumption Estimation and Momentary Power Consumption Profile Generation of a Softcore Processor**
Kula Y. F., Örs Yalçın S. B.
7th International Conference on Digital Information Processing and Communications (ICDIPC), Trabzon, Turkey, 2 - 04 May 2019, pp.41-46

V. **Model based node design methodology for secure IoT applications [Guvenli IoT uygulamalari için model tabanli düğum tasarimi yöntemi]**
özkaya ö., ÖRS YALÇIN S. B.
26th IEEE Signal Processing and Communications Applications Conference, SIU, 19 - 21 May 2018, pp.1-4

VI. **Electromagnetic radiation analysis of implementation of RSA algorithm on a Raspberry Pi [RSA Algoritmasinin Raspberry Pi Üzerinde Gerçeklemesine Elektromanyetik Yayinim Analizi]**
hatun e., büyükkaya e., ÖRS YALÇIN S. B.
26th IEEE Signal Processing and Communications Applications Conference, SIU, 19 - 21 May 2018, pp.1-4

VII. **Güvenli IoT Uygulamaları için Model Tabanlı Düğüm Tasarımı Yöntemi**
Özkaya Ö., Örs Yalçın S. B.
Signal Processing and Communications Applications Conference (SIU), İzmir, Turkey, 2 - 05 May 2018, pp.1

VIII. **RSA Algoritmasının Raspberry Pi Üzerinde Gerçeklemesine Elektromanyetik Yayınım Analizi**

Hatun E., Örs Yalçın S. B.
Signal Processing and Communications Applications Conference (SIU), İzmir, Turkey, 2 - 05 May 2018, pp.1

IX. **Karatsuba Ofman Multiplication Implementation on SystemC for Diffie-Hellman Key Exchange Algorithm**
AYGÜN S., KOUHALVANDİ L., ÖRS YALÇIN S. B., GÜNEŞ E. O.
4th International Conference on Knowledge-Based Engineering and Innovation (KBEI-2017), Tahran, Iran, 22 December 2017, pp.1-4

X. **Hardware/Software Co-Design of a Lightweight Crypto Algorithm BORON on an FPGA**
Acar B., Ors B.
10th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 30 November - 02 December 2017, pp.1272-1276

XI. **A Novel Template-based Multimedia Processor Array and Its Toolset**
Tukel M., YURDAKUL A., Ors B.
10th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 30 November - 02 December 2017, pp.437-441

XII. **Design and Implementation of an OpenRISC System-on-Chip with an Encryption Peripheral**
Akçay L., Tukel M., Ors B.
European Conference on Circuit Theory and Design (ECCTD), Catania, Italy, 4 - 06 September 2017

XIII. **Backhaul Infrastructures in Building Automation Systems Wired or Wireless**
Selahattin G., KARABULUT KURT G. Z., ÖRS YALÇIN S. B.
3rd IEEE IDAACS Symposium on WirelessSystems (IEEE IDAACS-SWS2016), 26 - 27 September 2017

XIV. **The Walsh-Hadamard Transform Based Automated Grading System For Monitoring of Heart Murmurs**
ARSLAN A., Bagbaba A. Ç., SEN B., Ors B.
National Conference on Electrical, Electronics and Biomedical Engineering (ELECO), Bursa, Turkey, 1 - 03 December 2016, pp.481-485

XV. **Design of an Emergency Building Evacuation System**
Gokceli S., Zhmurov N., Karabulut Kurt G. Z., Yalcin B. O.
National Conference on Electrical, Electronics and Biomedical Engineering (ELECO), Bursa, Turkey, 1 - 03 December 2016, pp.178-182

XVI. **Reliability analysis of MIPS-32 microprocessor register files designed with different fault tolerant techniques Farkli Hata Bagisiklilik Yöntemleri ile Tasarlanan MIPS-32 Mikroislemcisindeki Kaydedici Dosyasinin Güvenilirlik Analizleri**
Ustaoglu B., Yalcin B. O.
24th Signal Processing and Communication Application Conference, SIU 2016, Zonguldak, Turkey, 16 - 19 May 2016, pp.2073-2076

XVII. **Implementation of Enigma Machine Using Verilog on an FPGA**
Engin D., Ors B.
9th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 26 - 28 November 2015, pp.945-948

XVIII. **Data Hiding Method Using Image Interpolation And Pixel Symmetry**
Esen U., Ors B.
9th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 26 - 28 November 2015, pp.776-779

XIX. **A Layered UVM Based Testbench Design for SpaceWire**
Bagbaba A. Ç., Ustaoglu B., Erdem I., Ors B.
9th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 26 - 28 November 2015, pp.1164-1168

XX. **Implementation of an Indoor Localization Algorithms on an FPGA**
Azbar O., Ors B., Kurt G. K.
9th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 26 - 28 November

2015, pp.949-952

XXI. **Hardware Implementation of Novel Image Compression-Encryption System on a FPGA**
Bagbaba A. Ç., Ors B.
9th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 26 - 28 November 2015, pp.1159-1163

XXII. **Data transmission via GSM voice channel for end to end security**
OZKAN M. A., Ors S. B.
5th IEEE International Conference on Consumer Electronics - Berlin, ICCE-Berlin 2015, Berlin, Germany, 6 - 09 September 2015, pp.378-382

XXIII. **Application specific processor design for DCT based applications DCT Tabanli Uygulamar Için Uygulamaya Özel Işlemci Tasarimi**
Erozan A. T., Aydoıdu A. S., Örs B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Turkey, 16 - 19 May 2015, pp.2157-2160

XXIV. **Implementation of a modem which transmits digital data on GSM voice channel GSM Ses Kanalindan Sayisal Veri Ileten Bir Modemin Gerçeklenmesi**
POSTALLI H. S., TUNCAY S., Ors B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Turkey, 16 - 19 May 2015, pp.2537-2540

XXV. **Hardware / software codesign and implementation for secure NFC applications NFC ile Güvenli Uygulamalar için Donanim / Yazilim Ortak Sistem Tasarimi ve Gerçeklenmesi**
BASKIR S. G., Ors B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Turkey, 16 - 19 May 2015, pp.2392-2395

XXVI. **Creating Test Environment with UVM for SPI**
Ustaoglu B., Bagbaba A. C., Ors B., Erdem I.
23nd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16 - 19 May 2015, pp.2373-2376

XXVII. **JPEG Image Encryption via TEA Algorithm**
Bagbaba A. Ç., Ors B., KAYHAN O. S., EROZAN A. T.
23nd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16 - 19 May 2015, pp.2090-2093

XXVIII. **Design and Implementation of a Custom Verification Environment for Fault Injection and Analysis on an Embedded Microprocessor**
Ustaoglu B., Ors B.
3rd International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Beirut, Lebanon, 29 April - 01 May 2015, pp.256-261

XXIX. **Bina Yonetim Sistemleri icin Tahliye Modeli**
Taş B., Örs Yalçın S. B., KURT G. K.
Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Turkey, 4 - 05 December 2014, pp.1-5

XXX. **Leon3 Tabanli SoPC Tasarimi ve Uygulama Gerceklenmesi**
Bağbaba A. Ç., Ustaoglu B., Örs Yalçın S. B., Işık G., Erdem I.
Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Turkey, 4 - 05 December 2014, pp.1-5

XXXI. **Mikroislemci Tabanli Bir Sisteme Hata Enjekte Etme Yontemi Gelistirilmesi ve Hata Tespit Mekanizmasinin Gerceklenmesi**
Ustaoğlu B., Örs Yalçın S. B.
Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, Bursa, Turkey, 27 - 30 November 2014, pp.1-5

XXXII. **Image Filtering Processor and Its Applications**
Bagbaba A. Ç., Ors B., Erozan A. T.
22nd IEEE Signal Processing and Communications Applications Conference (SIU), Trabzon, Turkey, 23 - 25 April 2014, pp.2011-2014

XXXIII. **Implementation of a Secure Near Field Communication System on a FPGA**
Bagbaba A. Ç., Ors B.
8th International Conference on Electrical and Electronics Engineering (ELECO), Bursa, Turkey, 28 - 30 November 2013, pp.621-625

XXXIV. **System Level Design of Scalable Encryption Algorithm by Using CoWare**
ALTINTAS A., Ors B.
International Conference on Computer, Information and Telecommunication Systems (CITS), Athens, Greece, 7 - 08 May 2013

XXXV. **Design and Implementation of a Secure RFID System on FPGA**
Ozen O. E., Örs Yalçın S. B., Yağcı H. B.
21st Signal Processing and Communications Applications Conference (SIU), CYPRUS, 24 - 26 April 2013

XXXVI. **Reed-solomon decoder hardware implementation for DVB-S receiver DVB-S alicisi için reed-solomon kod çözücü donanim gerçeklemesi**
DILEK S. M., Örs B., Kartal M.
2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Turkey, 24 - 26 April 2013

XXXVII. **Reed Solomon Decoder Hardware Implementation for DVB S Receiver**
DİLEK S. M., ÖRS YALÇIN S. B., KARTAL M.
21st Signal Processing and Communications Applications Conference, Girne, Cyprus (Kktc), 24 - 26 April 2013

XXXVIII. **Hardware/Software Codesign for Watermarking in DCT Domain**
Erozan A. T., Baskir S. G., Ors B.
21st Signal Processing and Communications Applications Conference (SIU), CYPRUS, 24 - 26 April 2013

XXXIX. **Hardware/software codesign for watermarking in DCT domain DCT tanim kumesindeki damgalama islemleri icin yazilim/donanim ortakli sistem tasarimi**
EROZAN A. T., BASKIR S. G., Ors B.
2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Turkey, 24 - 26 April 2013

XL. **Implementation of a Secure RFID Protocol**
Baskir S. G., Ors B.
21st Signal Processing and Communications Applications Conference (SIU), CYPRUS, 24 - 26 April 2013

XLI. **Implementation of a secure RFID protocol Güvenli bir RFID protokolünün gerçeklenmesi**
BASKIR S. G., Ors B.
2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Turkey, 24 - 26 April 2013

XLII. **Design and implementation of a secure RFID system on FPGA Güvenli bir RFID sisteminin FPGA üzerinde tasarimi ve gerçeklenmesi**
ÖZEN O. E., Berna Örs S. B., Bülent Yağci H.
2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Turkey, 24 - 26 April 2013

XLIII. **Guvenli RFID Sistemleri Icin Bir Kimlik Dogrulama Protokolnun Gerceklenmesi**
Alparslan S., Örs Yalçın S. B.
Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Turkey, 29 - 30 November 2012, pp.1-5

XLIV. **Kriptoloji Uygulamalarina Ozel Bir Islemcinin Tasarlanarak FPGA Uzerinde Gerceklenmesi**
Şahin O., Örs Yalçın S. B.
Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Turkey, 29 - 30 November 2012, pp.1-5

XLV. **GSM Ses Kanalindan Sayisal Veri ileten Bir Modemin Tasarimi ve Gerceklenmesi**
Tuncay S., Özkan A., Örs Yalçın S. B.
Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Turkey, 29 - 30 November 2012, pp.1-5

XLVI. **Architectures for fast modular multiplication**
Aris A., Ors B., Saldamli G.
2011 14th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, DSD 2011, Oulu,

Finland, 31 August - 02 September 2011, pp.434-437

XLVII. **System Level Design of a Secure Healthcare Smart Card System**
OKSAR M., Ors B., Saldamli G.
IEEE Systems and Information Engineering Design Symposium (SIEDS), Virginia, United States Of America, 29 April 2011, pp.170-175

XLVIII. **Implementation of a PUF circuit on a FPGA**
SOYBALI M., Ors B., Saldamli G.
4th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2011, Paris, France, 7 - 10 February 2011

XLIX. **Analyzing and comparing the Montgomery multiplication algorithms for their power consumption**
BAYHAN D., Ors S. B., SALDAMLI G.
6th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 30 November - 01 December 2010, pp.257-261

L. **DESIGN OF NEW TINY CIRCUITS FOR AES ENCRYPTION ALGORITHM**
DALMISLI K. V., Ors B.
3rd International Conference on Signals, Circuits and Systems, Medenine, Tunisia, 6 - 08 November 2009, pp.565-569

LI. **Differential Power Analysis Attack Considering Decoupling Capacitance Effect**
Danis A. U., Ors B.
European Conference on Circuit Theory Design, Antalya, Turkey, 23 - 27 August 2009, pp.359-360

LII. **RFID Sistemlerinin Mikroislemci Uzerinde Guvenli Olacak Sekilde Gerceklenmesi**
Bulut K., Örs Yalçın S. B., Yavuz İ.
3. Uluslararasi Katilimli Bilgi Guvenligi ve Kriptoloji Konferansi, Ankara, Turkey, 25 - 27 December 2008, pp.1-5

LIII. **Bir Steganografi Sisteminin FPGA Uzerinde Gerceklenmesi**
Elçi B., Örs Yalçın S. B., DALMISLI K. V.
3. Uluslararasi Katilimli Bilgi Guvenligi ve Kriptoloji Konferansi, Ankara, Turkey, 25 - 27 December 2008, pp.1-5

LIV. **FPGA implementation of an elliptic curve cryptosystem over GF(3 m)**
Yavuz I., Yalçin S. B., Koç Ç. K.
2008 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2008, Cancun, Mexico, 3 - 05 December 2008, pp.397-402

LV. **Gelismis Sifreleme Standardinin - AES - FPGA Uzerinde Gerceklenmesi**
DALMISLI K. V., Örs Yalçın S. B.
Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, Bursa, Turkey, 26 - 30 November 2008, pp.1-5

LVI. **Differential Power Analysis resistant hardware implementation of the RSA cryptosystem**
Bayam K. A., Ors B.
IEEE International Symposium on Circuits and Systems, Washington, United States Of America, 18 - 21 May 2008, pp.3314-3315

LVII. **Power analysis resistant hardware implementations of AES**
ORDU L., Örs B.
14th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2007, Marrakech, Morocco, 11 - 14 December 2007, pp.1408-1411

LVIII. **Differential electromagnetic attack on an fpga implementation of elliptic curve cryptosystems**
DE MULDER E., Örs S. B., PRENEEL B., VERBAUWHEDE I.
2006 World Automation Congress, WAC'06, Budapest, Hungary, 24 - 26 June 2006

LIX. **Serial multiplier architectures over GF(2(n)) for elliptic curve cryptosystems**
BATINA L., MENTENS N., Ors S. B., PRENEEL B.
12th IEEE Mediterranean Electrotechnical Conference (MELECON 2004), Dubrovnik, Croatia, 12 - 15 May 2004, pp.779-782

LX. **An FPGA Implementation of an EllipticCurve Processor over GF(2^m)**
MENTENS N., Örs Yalçın S. B., PRENEEL B.
the 2004 Great Lakes Symposiumon VLSI (GLSVLSI 2004), Boston, United States Of America, 26 - 28 April 2004,

pp.454-457

LXI. **Power-analysis attack on an ASIC AES implementation**
Ors S. B., GURKAYNAK F. K., OSWALD E., PRENEEL B.
International Conference on Information Technology - Coding and Computing, Nevada, United States Of America, 5 - 07 April 2004, pp.546-552

LXII. **Power-Analysis Attacks on an FPGA -- First Experimental Results**
Örs Yalçın S. B., OSWALD E., PRENEEL B.
the 5th International Workshop on Cryptographic Hardware and Embedded Systems (CHES), Köln, Germany, 8 - 10 September 2003, pp.35-50

LXIII. **Hardware implementation of an elliptic curve processor over GF(p)**
Örs S. B., Batina L., PRENEEL B., VANDEWALLE J.
IEEE International Conference on Application-Specific Systems, Architectures, and Processors, ASAP 2003, The Hague, Netherlands, 24 - 26 June 2003, pp.433-443

LXIV. **Hardware implementation of a Montgomery modular multiplier in a systolic array**
Örs S. B., Batina L., PRENEEL B., VANDEWALLE J.
International Parallel and Distributed Processing Symposium, IPDPS 2003, Nice, France, 22 - 26 April 2003

LXV. **Modeling n/spl times/n bit multiplication blocks for DSP applications using VHDL**
Ors S. B., DERVISOGLU A.
25th EUROMICRO Conference on Informatics: Theory and Practice for the New Millennium, EUROMICRO 1999, Milan, Italy, 8 - 10 September 1999, vol.1, pp.402-405

Supported Projects

Örs Yalçın S. B., Project Supported by Higher Education Institutions, Reliability And Securty of Arbiter Based Physical Unclonable function Circuits, 2013 - 2018
Örs Yalçın S. B., Project Supported by Higher Education Institutions, Differential Power Analysis Resistant Hardware Implementation of the RSA Cryptoayste, 2008 - 2018
Örs Yalçın S. B., Project Supported by Higher Education Institutions, Eliptik Eğri Kripto Sistemlerinin FPGA Gerçeklemeleri Üzerinde Elektromagnetik Yayınım Analizi Saldırısı, 2006 - 2018
Örs Yalçın S. B., Project Supported by Higher Education Institutions, Kriptografi Algoritmaları İçin Gömülü Sistem Tasarımı, 2006 - 2008
Örs Yalçın S. B., Project Supported by Higher Education Institutions, AES Şifreleme Algoritmasının Yan Kanal Ataklarına Karşı Güvenli Olacak Şekilde FPGA Üzerinde Gerçeklenmesi, 2006 - 2007

Metrics

Publication: 118
Citation (WoS): 365
Citation (Scopus): 704
H-Index (WoS): 8
H-Index (Scopus): 12

Non Academic Experience

Business Establishment Private, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe Güvenpark
Business Establishment Private, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe
Business Establishment Private, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe

Türk Akreditasyon Kurumu
Business Establishment Private, Neta Elektronik. A.Ş., Arge
NETA Elektronik A.Ş.
Defne Telekomunikasyon A.Ş.
Eczacibasi Bilisim A.Ş.
University of California San Diego
Katholieke Universiteit Leuven