

Prof.Dr. Sıddıka Berna Örs Yalçın

Kişisel Bilgiler

Fax Telefonu: [+90 212 285 3565](tel:+902122853565)

E-posta: orssi@itu.edu.tr

Web: <http://web.itu.edu.tr/~orssi/>

Posta Adresi: İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Maslak, İstanbul

Uluslararası Araştırmacı ID'leri

ORCID: 0000-0003-0851-8501

Publons / Web Of Science ResearcherID: D-8397-2013

ScopusID: 6602685919

Yoksis Araştırmacı ID: 149119

Eğitim Bilgileri

Doktora, Katholieke Universiteit Leuven, Uygulamalı Bilimler, Belçika 1999 - 2005

Yüksek Lisans, İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, Türkiye 1995 - 1998

Lisans, İstanbul Teknik Üniversitesi, Elektrik-Elektronik Mühendisliği Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, Türkiye 1991 - 1995

Yabancı Diller

İngilizce

Yaptığı Tezler

Doktora, HARDWARE DESIGN OF ELLIPTIC CURVE CRYPTOSYSTEMS AND SIDE-CHANNEL ATTACKS, Katholieke Universiteit Leuven, Faculteit Toegepaste Wetenschappen, Departement Elektrotechniek, 2005

Yüksek Lisans, Design of Multiplier Blocks for DSP Applications Using VHDL, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Ve Haberleşme Mühendisliği Bölümü, 1995

Araştırma Alanları

Teknik Bilimler, Bilgisayar Bilimleri, Bilgi Güvenliği ve Güvenilirliği, Donanım, Elektrik-Elektronik Mühendisliği, Elektronik, Elektronik Devreler

Akademik Unvanlar / Görevler

Prof.Dr., İstanbul Teknik Üniversitesi, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2020 - Devam Ediyor

Doç.Dr., İstanbul Teknik Üniversitesi, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2011 - 2020

Doç.Dr., Bahçeşehir Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, 2017 - 2018

Doç.Dr., Yeditepe Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği, 2012 - 2015

Yrd.Doç.Dr., İstanbul Teknik Üniversitesi, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 2005 - 2011
Öğretim Görevlisi Dr., University of California, San Diego, Computer Science And Engineering, 2009 - 2009
Araştırma Görevlisi, Katholieke Universiteit Leuven, Engineering, Electrical Engineering, 1999 - 2005
Araştırma Görevlisi, İstanbul Teknik Üniversitesi, Elektrik-Elektronik, Elektronik Ve Haberleşme Mühendisliği, 1995 - 2005

Verdiği Dersler

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

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- I. **New lightweight mitigation techniques for RPL version number attacks**
Arış A., Yalcin S. B., Oktuğ S. F.
AD HOC NETWORKS, cilt.85, ss.81-91, 2019 (SCI-Expanded)
- II. **Customizable embedded processor array for multimedia applications**
Tükel M., Yurdakul A., Ors B.
INTEGRATION-THE VLSI JOURNAL, cilt.60, ss.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, cilt.25, sa.2, ss.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, cilt.12, sa.10, ss.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, cilt.26, sa.6, ss.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, cilt.18, sa.1, ss.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, cilt.33, ss.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, cilt.3203, ss.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, cilt.23, ss.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, cilt.3156, ss.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, cilt.34, ss.1-64, 2003 (SCI-Expanded)

Diğer Dergilerde Yayınlanan Makaleler

- 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, cilt.3, sa.4, ss.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, cilt.4, ss.36-45, 2004 (Hakemli Dergi)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- I. **System on Chip Design with Vivado High-Level Synthesis Tool**
Bilgili B., Yamaneren C., Vatansver K., Çoltu U., ÖRS YALÇIN S. B.
11th INTERNATIONAL CONFERENCE on ELECTRICAL and ELECTRONICS ENGINEERING, 28 - 30 Kasım 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, Türkiye, 28 - 30 Kasım 2019, ss.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, Türkiye, 24 - 26 Nisan 2019, ss.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, Türkiye, 2 - 04 Mayıs 2019, ss.41-46
- V. **Model based node design methodology for secure IoT applications [Güvenli IoT uygulamaları için model tabanlı düğüm tasarımı yöntemi]**
Özkaya Ö., ÖRS YALÇIN S. B.
26th IEEE Signal Processing and Communications Applications Conference, SIU, 19 - 21 Mayıs 2018, ss.1-4
- VI. **Electromagnetic radiation analysis of implementation of RSA algorithm on a Raspberry Pi [RSA Algoritmasının Raspberry Pi Üzerinde Gerçeklemesine Elektromanyetik Yayınım Analizi]**
hatun e., büyükkaya e., ÖRS YALÇIN S. B.
26th IEEE Signal Processing and Communications Applications Conference, SIU, 19 - 21 Mayıs 2018, ss.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, Türkiye, 2 - 05 Mayıs 2018, ss.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, Türkiye, 2 - 05 Mayıs 2018, ss.1

- IX. Karatsuba Ofman Multiplication Implementation on SystemC for Diffie-Hellman Key Exchange Algorithm**
AYGÜN S., KOUHALVANDI L., ÖRS YALÇIN S. B., GÜNEŞ E. O.
4th International Conference on Knowledge-Based Engineering and Innovation (KBEI-2017), Tahran, İran, 22 Aralık 2017, ss.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, Türkiye, 30 Kasım - 02 Aralık 2017, ss.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, Türkiye, 30 Kasım - 02 Aralık 2017, ss.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, İtalya, 4 - 06 Eylül 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 Eylül 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, Türkiye, 1 - 03 Aralık 2016, ss.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, Türkiye, 1 - 03 Aralık 2016, ss.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, Türkiye, 16 - 19 Mayıs 2016, ss.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, Türkiye, 26 - 28 Kasım 2015, ss.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, Türkiye, 26 - 28 Kasım 2015, ss.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, Türkiye, 26 - 28 Kasım 2015, ss.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, Türkiye, 26 - 28 Kasım 2015, ss.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, Türkiye, 26 - 28 Kasım 2015, ss.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, Almanya, 6 - 09 Eylül 2015, ss.378-382
- XXIII. **Application specific processor design for DCT based applications DCT Tabanlı Uygulamalar İçin Uygulamaya Özel İşlemci Tasarımı**
Erozan A. T., Aydoğdu A. S., Örs B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Türkiye, 16 - 19 Mayıs 2015, ss.2157-2160
- XXIV. **Implementation of a modem which transmits digital data on GSM voice channel GSM Ses Kanalından Sayısal Veri İleten Bir Modemin Gerçeklenmesi**
POSTALLI H. S., TUNCAY S., Ors B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Türkiye, 16 - 19 Mayıs 2015, ss.2537-2540
- XXV. **Hardware / software codesign and implementation for secure NFC applications NFC ile Güvenli Uygulamalar için Donanım / Yazılım Ortak Sistem Tasarımı ve Gerçeklenmesi**
BASKIR S. G., Ors B.
2015 23rd Signal Processing and Communications Applications Conference, SIU 2015, Malatya, Türkiye, 16 - 19 Mayıs 2015, ss.2392-2395
- XXVI. **Creating Test Environment with UVM for SPI**
Ustaoglu B., Bagbaba A. C., Ors B., Erdem I.
23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Türkiye, 16 - 19 Mayıs 2015, ss.2373-2376
- XXVII. **JPEG Image Encryption via TEA Algorithm**
Bagbaba A. Ç., Ors B., KAYHAN O. S., EROZAN A. T.
23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Türkiye, 16 - 19 Mayıs 2015, ss.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 (TAECE), Beirut, Lübnan, 29 Nisan - 01 Mayıs 2015, ss.256-261
- XXIX. **Bina Yönetim Sistemleri için Tahliye Modeli**
Taş B., Örs Yalçın S. B., KURT G. K.
Gomulu Sistemler ve Uygulamaları Sempozyumu (GomSis), İstanbul, Türkiye, 4 - 05 Aralık 2014, ss.1-5
- XXX. **Leon3 Tabanlı SoPC Tasarımı ve Uygulama Gerçeklenmesi**
Bağbaba A. Ç., Ustaoglu B., Örs Yalçın S. B., Işık G., Erdem I.
Gomulu Sistemler ve Uygulamaları Sempozyumu (GomSis), İstanbul, Türkiye, 4 - 05 Aralık 2014, ss.1-5
- XXXI. **Mikroişlemci Tabanlı Bir Sisteme Hata Enjekte Etme Yöntemi Geliştirilmesi ve Hata Tespit Mekanizmasının Gerçeklenmesi**
Ustaoglu B., Örs Yalçın S. B.
Elektrik - Elektronik Ve Bilgisayar Mühendisliği Sempozyumu, Bursa, Türkiye, 27 - 30 Kasım 2014, ss.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, Türkiye, 23 - 25 Nisan 2014, ss.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, Türkiye, 28 - 30 Kasım 2013, ss.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, Yunanistan, 7 - 08 Mayıs 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 Nisan 2013

XXXVI. Reed-solomon decoder hardware implementation for DVB-S receiver DVB-S alicisi için reed-solomon kod çözücü donanım gerçekleştirilmesi

DİLEK S. M., Örs B., Kartal M.

2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Türkiye, 24 - 26 Nisan 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, Kıbrıs (Kktc), 24 - 26 Nisan 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 Nisan 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, Türkiye, 24 - 26 Nisan 2013

XL. Implementation of a Secure RFID Protocol

Baskir S. G., Ors B.

21st Signal Processing and Communications Applications Conference (SIU), CYPRUS, 24 - 26 Nisan 2013

XLI. Implementation of a secure RFID protocol Güvenli bir RFID protokolünün gerçekleştirilmesi

BASKIR S. G., Ors B.

2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Türkiye, 24 - 26 Nisan 2013

XLII. Design and implementation of a secure RFID system on FPGA Güvenli bir RFID sisteminin FPGA üzerinde tasarimi ve gerçekleştirilmesi

ÖZEN O. E., Berna Örs S. B., Bülent Yağcı H.

2013 21st Signal Processing and Communications Applications Conference, SIU 2013, Haspolat, Türkiye, 24 - 26 Nisan 2013

XLIII. Güvenli RFID Sistemleri İçin Bir Kimlik Doğrulama Protokolünün Gerçekleştirilmesi

Alparslan S., Örs Yalçın S. B.

Gomulu Sistemler ve Uygulamaları Sempozyumu (GomSis), İstanbul, Türkiye, 29 - 30 Kasım 2012, ss.1-5

XLIV. Kriptoloji Uygulamalarına Özel Bir İşlemcinin Tasarlanarak FPGA Üzerinde Gerçekleştirilmesi

Şahin O., Örs Yalçın S. B.

Gomulu Sistemler ve Uygulamaları Sempozyumu (GomSis), İstanbul, Türkiye, 29 - 30 Kasım 2012, ss.1-5

XLV. GSM Ses Kanalından Sayısal Veri İleten Bir Modemin Tasarımı ve Gerçekleştirilmesi

Tuncay S., Özkan A., Örs Yalçın S. B.

Gomulu Sistemler ve Uygulamaları Sempozyumu (GomSis), İstanbul, Türkiye, 29 - 30 Kasım 2012, ss.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, Finlandiya, 31 Ağustos - 02 Eylül 2011, ss.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, Amerika Birleşik Devletleri, 29 Nisan 2011, ss.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, Fransa, 7 - 10 Şubat 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, Mısır, 30 Kasım - 01 Aralık 2010, ss.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, Tunus, 6 - 08 Kasım 2009, ss.565-569

LI. Differential Power Analysis Attack Considering Decoupling Capacitance Effect

Danis A. U., Ors B.

European Conference on Circuit Theory Design, Antalya, Türkiye, 23 - 27 Ağustos 2009, ss.359-360

LII. RFID Sistemlerinin Mikroislemci Uzerinde Guvenli Olacak Sekilde Gercekleenmesi

Bulut K., Örs Yalçın S. B., Yavuz İ.

3. Uluslararası Katılımlı Bilgi Guvenligi ve Kriptoloji Konferansi, Ankara, Türkiye, 25 - 27 Aralık 2008, ss.1-5

LIII. Bir Steganografi Sisteminin FPGA Uzerinde Gercekleenmesi

Elçi B., Örs Yalçın S. B., DALMISLI K. V.

3. Uluslararası Katılımlı Bilgi Guvenligi ve Kriptoloji Konferansi, Ankara, Türkiye, 25 - 27 Aralık 2008, ss.1-5

LIV. FPGA implementation of an elliptic curve cryptosystem over GF(3 m)

Yavuz I., Yalçın S. B., Koç Ç. K.

2008 International Conference on Reconfigurable Computing and FPGAs, ReConFig 2008, Cancun, Meksika, 3 - 05 Aralık 2008, ss.397-402

LV. Gelismis Sifreleme Standardinin - AES - FPGA Uzerinde Gercekleenmesi

DALMISLI K. V., Örs Yalçın S. B.

Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, Bursa, Türkiye, 26 - 30 Kasım 2008, ss.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, Amerika Birleşik Devletleri, 18 - 21 Mayıs 2008, ss.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, Fas, 11 - 14 Aralık 2007, ss.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, Macaristan, 24 - 26 Haziran 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, Hırvatistan, 12 - 15 Mayıs 2004, ss.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 Symposium on VLSI (GLSVLSI 2004), Boston, Amerika Birleşik Devletleri, 26 - 28 Nisan 2004, ss.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, Amerika Birleşik Devletleri, 5 - 07 Nisan 2004, ss.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, Almanya, 8 - 10 Eylül 2003, ss.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, Hollanda, 24 - 26 Haziran 2003, ss.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, Fransa, 22 - 26 Nisan 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, İtalya, 8 - 10 Eylül 1999, cilt.1, ss.402-405

Desteklenen Projeler

Örs Yalçın S. B., Yükseköğretim Kurumları Destekli Proje, Reliability And Securty of Arbiter Based Physical Unclonable function Circuits, 2013 - 2018

Örs Yalçın S. B., Yükseköğretim Kurumları Destekli Proje, Differential Power Analysis Resistant Hardware Implementation of the RSA Cryptoayste, 2008 - 2018

Örs Yalçın S. B., Yükseköğretim Kurumları Destekli Proje, Eliptik Eğri Kripto Sistemlerinin FPGA Gerçeklemeleri Üzerinde Elektromagnetik Yayınım Analizi Saldırısı, 2006 - 2018

Örs Yalçın S. B., Yükseköğretim Kurumları Destekli Proje, Kriptografi Algoritmaları İçin Gömülü Sistem Tasarımı, 2006 - 2008

Örs Yalçın S. B., Yükseköğretim Kurumları Destekli Proje, AES Şifreleme Algoritmasının Yan Kanal Ataklarına Karşı Güvenli Olacak Şekilde FPGA Üzerinde Gerçeklenmesi, 2006 - 2007

Metrikler

Yayın: 118

Atıf (WoS): 365

Atıf (Scopus): 704

H-İndeks (WoS): 8

H-İndeks (Scopus): 12

Akademi Dışı Deneyim

Ticari Kuruluş Özel, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe Güvenpark

Ticari Kuruluş Özel, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe

Ticari Kuruluş Özel, GÜVENPARK BİLİŞİM TEKNOLOJİLERİ ARAŞTIRMA VE GELİŞTİRME TİC. LTD. ŞTİ., ArGe

Türk Akreditasyon Kurumu

Ticari Kuruluş Özel, 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