Doç.Dr. Sıddıka Berna Örs Yalçın

Kişisel Bilgiler

Fax Telefonu: +90 212 285 3565
E-posta: orssi@itu.edu.tr
Web: http://web.itu.edu.tr/~orssi/
Posta Adresi: İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Maslak, İstanbul

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, Faculteıt Toegepaste Wetenschappen, Departement Elektrotechnıek, 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

Doç.Dr., Bahçeşehir Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği, 2017 - Devam Ediyor
Doç.Dr., İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, 2011 - Devam Ediyor
Doç.Dr., Yeditepe Üniversitesi, Mühendislik Fakültesi, Elektrik-Elektronik Mühendisliği, 2012 - 2015
Yrd.Doç.Dr., İstanbul Teknik Üniversitesi, Elektrik-Elektronik Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, 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 Fakültesi, Elektronik Ve Haberleşme Mühendisliği Bölümü, 1995 - 2005

Mesleki Deneyim

Verdiği Dersler

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

SCI, SSCI ve AHCI İndekslerine Giren Dergilerde Yayınlanan Makaleler

- **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 İndekslerine Giren Dergi)
- **Customizable embedded processor array for multimedia applications**
  Tükel M., Yurdakul A., Ors B.
  INTEGRATION-THE VLSI JOURNAL, cilt.60, ss.213-223, 2018 (SCI İndekslerine Giren Dergi)
- **Analyzing and comparing the AES architectures for their power consumption**
  DOGAN A., Ors S. B. , Saldamli G.
  JOURNAL OF INTELLIGENT MANUFACTURING, cilt.25, ss.263-271, 2014 (SCI İndekslerine Giren Dergi)
- **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, ss.2037-2049, 2013 (SCI İndekslerine Giren Dergi)
- **Reliability and security of arbiter-based physical unclonable function circuits**
  TARIGULIYEV Z., Ors B.
  INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, cilt.26, ss.757-769, 2013 (SCI İndekslerine Giren Dergi)
- **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, ss.129-140, 2010 (SCI İndekslerine Giren Dergi)
- **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 İndekslerine Giren Dergi)
- **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 İndekslerine Giren Dergi)
- **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 İndekslerine Giren Dergi)
- **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 İndekslerine Giren Dergi)

- **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 İndekslerine Giren Dergi)

Diğer Dergilerde Yayınlanan Makaleler

- **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, ss.229-240, 2008 (Diğer Kurumların Hakemli Dergileri)
- **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 (Diğer Kurumların Hakemli Dergileri)

Hakemli Kongre / Sempozyum Bildiri Kitaplarında Yer Alan Yayınlar

- **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 Kasım 2019
- **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
- **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
- **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
- **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 Mayıs 2018, ss.1-4
- **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 Mayıs 2018, ss.1-4
- **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
- **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
- **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, İran, 22 Aralık 2017, ss.1-4

- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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
- **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

- **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
- **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, Türkiye, 16 - 19 Mayıs 2015, ss.2157-2160
- **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, Türkiye, 16 - 19 Mayıs 2015, ss.2537-2540
- **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, Türkiye, 16 - 19 Mayıs 2015, ss.2392-2395
- **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, Türkiye, 16 - 19 Mayıs 2015, ss.2373-2376
- **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, Türkiye, 16 - 19 Mayıs 2015, ss.2090-2093
- **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, Lübnan, 29 Nisan - 01 Mayıs 2015, ss.256-261
- **Bina Yonetim Sistemleri icin Tahliye Modeli**
  Taş B., Örs Yalçın S. B. , KURT G. K.
  Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Türkiye, 4 - 05 Aralık 2014, ss.1-5
- **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, Türkiye, 4 - 05 Aralık 2014, ss.1-5
- **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, Türkiye, 27 - 30 Kasım 2014, ss.1-5
- **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
- **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

- **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
- **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
- **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, Türkiye, 24 - 26 Nisan 2013
- **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
- **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
- **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
- **Implementation of a Secure RFID Protocol**
  Baskir S. G. , Ors B.
  21st Signal Processing and Communications Applications Conference (SIU), CYPRUS, 24 - 26 Nisan 2013
- **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, Türkiye, 24 - 26 Nisan 2013
- **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, Türkiye, 24 - 26 Nisan 2013
- **Guvenli RFID Sistemleri Icin Bir Kimlik Dogrulama Protokolnun Gerceklenmesi**
  Alparslan S., Örs Yalçın S. B.
  Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Türkiye, 29 - 30 Kasım 2012, ss.1-5
- **Kriptoloji Uygulamalarina Ozel Bir Islemcinin Tasarlanarak FPGA Uzerinde Gerceklenmesi**
  Şahin O., Örs Yalçın S. B.
  Gomulu Sistemler ve Uygulamalari Sempozyumu (GomSis), İstanbul, Türkiye, 29 - 30 Kasım 2012, ss.1-5
- **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, Türkiye, 29 - 30 Kasım 2012, ss.1-5
- **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
- **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
- **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
- **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
- **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
- **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
- **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, Türkiye, 25 - 27 Aralık 2008, ss.1-5
- **Bir Steganografi Sisteminin FPGA Uzerinde Gerceklenmesi**
  Elçi B., Örs Yalçın S. B. , DALMISLI K. V.
  3. Uluslararasi Katilimli Bilgi Guvenligi ve Kriptoloji Konferansi, Ankara, Türkiye, 25 - 27 Aralık 2008, ss.1-5
- **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, Meksika, 3 - 05 Aralık 2008, ss.397-402
- **Gelismis Sifreleme Standardinin - AES - FPGA Uzerinde Gerceklenmesi**
  DALMISLI K. V. , Örs Yalçın S. B.
  Elektrik - Elektronik Ve Bilgisayar Muhendisligi Sempozyumu, Bursa, Türkiye, 26 - 30 Kasım 2008, ss.1-5
- **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
- **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
- **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
- **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
- **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, Amerika Birleşik Devletleri, 26 - 28 Nisan 2004, ss.454-457
- **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

- **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
- **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
- **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
- **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

Atıflar

Toplam Atıf Sayısı (WOS):361
h-indeksi (WOS):8