

SESSION CHAIR:

Paris Kitsos
Hellenic Open University /
KNOSSOSnet Research Group,
Patras, Greece

SPECIAL SESSION PROGRAM SUBCOMMITTEE:

- Akashi Satoh,
National Institute of Advanced Industrial
Science and Technology, Japan

-Claudia Feregrino-Uribe,
INAOE, Mexico

-Francesco Loporati,
University of Pavia, Italy

-Jens-Peter Kaps
George Mason University, USA

- Jorge Guajardo,
Robert Bosch LLC,
Research and Technology Center, USA

- Lejla Batina,
Radboud University Nijmegen, The
Netherlands

- Máire O'Neill,
Queen's University Belfast, Ireland

-Nicolas Sklavos,
Technological Educational Institute of
Patras, Greece

-Odysseas Koufopavlou,
University of Patras, Greece

- Reouven Elbaz,
Intel, USA

- Steve Trimberger,
Xilinx, USA

-Tim Güneysu,
Ruhr University Bochum, Germany

-Thomas Plos,
Graz University of Technology, Austria

CONTACT INFORMATION

Dr. Paris Kitsos
School of Science & Technology
Hellenic Open University
13-15 Tsamadou str., Patras,
GR-26222, Greece
Phone : +30 2610 367535
Fax : +30 2610 367520
e-mail: pkitsos@eap.gr

SPECIAL SESSION ON ARCHITECTURES AND HARDWARE FOR SECURITY APPLICATIONS (AHSA)

The rapidly growth of the next generation communication systems, which enable the communications between mobile computers, phones and smart devices, the offering of new electronic commerce services make imperative the necessity for efficient and/or high performance implementations of security applications. The focus of this special session is on all aspects of cryptographic and security hardware systems

SPECIAL SESSION SCOPE

The scope of this special session is on all views of hardware-oriented security. This special session is a presentation for new results from both the research and industry communities. Special interests are contributions that describe new methods for secure and efficient hardware implementations for embedded systems, e.g. smart cards, microprocessors, DSPs, RFID and Wireless Sensor Networks, etc.

The topics of this special session include but are not limited to:

- Efficient hardware architectures for symmetric and asymmetric cryptographic algorithms
- Processors and co-processors for cryptography applications
- Processors for smart card security
- True and pseudorandom number generators
- Reconfigurable hardware for cryptography
- FPGA design security
- Physical unclonable functions and applications
- Trusted computing platforms
- Hardware architectures for cryptanalysis
- Security architectures for pervasive computing and wireless applications/protocols
- Lightweight implementations
- Implementation of cryptosystems and their integration into secure systems
- Applications of secure hardware
- All types of attacks against implementations
- Hardware trojans and trusted ICs

SUBMISSION GUIDELINES

Prospective authors are encouraged to submit their manuscripts for review electronically through the following web page (<http://www.easychair.org/conferences/?conf=dsd2012>) or by sending the paper to the Session Chair via email (pkitsos@eap.gr, only if an unexpected web access problem is encountered) before the deadline for submission.

Each manuscript should include the complete paper text, all illustrations, and references. The manuscript should conform to the required IEEE format: single-spaced, double column, A4/US letter page size, 10-point size Times Roman font, up to 8 pages. In order to conduct a blind review, no indication of the authors' names should appear in the submitted manuscript, references included.

The IEEE Conference Publishing Services (CPS), Conference Publishing Services, publishes the DSD Proceedings, which are available worldwide through the IEEE Xplore Digital Library. An extended version of the best papers will be published in a special issue of the ISI-indexed "Microprocessors and Microsystems: Embedded Hardware Design" journal, printed by Elsevier Ltd

IMPORTANT DATES

- Submission of papers: March 26th, 2012
- Notification of acceptance: May 7th, 2012
- Camera ready papers: May 31st, 2012

WEB LINKS

- DSD'12 web page:
- www.univ-valenciennes.fr/dsd2012
- Euromicro web page:
<http://www.euromicro.org>