Call for Papers / New Journal Announcement

Journal of Cryptographic Engineering

4 issues/year

ISSN 2190-8508 / e-ISSN 2190-8516

Aims & Scope

The Journal of Cryptographic Engineering is an archival journal publishing high-quality scientific articles presenting methods, techniques, tools, implementations, and applications of research in cryptographic engineering, including cryptographic hardware, cryptographic embedded systems, and embedded security. JCEEN aims to serve the academic and corporate R&D community interested in cryptographic hardware and embedded security by offering a focused journal drawing together archival papers that are presently scattered across various journals.

The Journal of Cryptographic Engineering will cover the research areas summarized below.

Cryptographic Hardware:

Hardware architectures for public-key cryptography and secret-key cryptography; special-purpose hardware for cryptanalysis; cryptographic processors and co-processors; hardware accelerators for security protocols (security processors, network processors, etc.); true and pseudorandom number generators; Physically Unclonable Functions (PUFs).

Cryptographic Software for Embedded Systems:

Efficient software implementations of cryptography for embedded processors; efficient and secure implementations of cryptography using multiprocessor cores; cryptographic libraries; cryptographic algorithms targeting embedded devices.

Attacks Against Implementations and Countermeasures Against These Attacks:

Side channel attacks and countermeasures; faults and fault models for cryptographic devices; fault attacks and countermeasures; hardware tamper resistance; Trojan hardware.

Tools and Methodologies:

Computer aided cryptographic engineering; methodologies and environments for fair comparison of hardware and software efficiency of cryptographic algorithms, architectures, and implementations; partial and run-time reconfiguration of cryptographic systems; reliability and fault tolerance in cryptography and cryptanalysis; architectures for trusted computing.

Applications and Implementation Environments:

Cryptography in wireless applications (mobile phone, WLANs, etc.); cryptography for pervasive computing (RFID, sensor networks, etc.); FPGA design security; hardware IP protection and anti-counterfeiting techniques; reconfigurable hardware for cryptography; smart card processors, systems, and applications; security in commercial consumer applications (pay-TV, automotive, etc.); secure storage devices (memories, disks, etc.); technologies and hardware for content protection; security for embedded software and systems.
Call for Papers / New Journal Announcement

Journal of Cryptographic Engineering

4 issues/year – ISSN 2190-8508 / e-ISSN 2190-8516

Editor-in-Chief
Çetin Kaya Koç,
University of California Santa Barbara, USA

Steering Committee
Çetin Kaya Koç, University of California Santa Barbara, USA
Christof Paar, Ruhr University of Bochum, Germany
Jean-Jacques Quisquater, Université Catholique de Louvain, Belgium
Ingrid Verbauwhede, Katholieke Universiteit Leuven, Belgium

Associate Editors
Paulo S.L. Barreto, University of Sao Paulo, Brazil
pbarreto@larc.usp.br
Lejla Batina, Radboud University Nijmegen, The Netherlands
Lejla.Batina@esat.kuleuven.be
Dan Bernstein, University of Illinois at Chicago, USA
djb@cr.yp.to
Guido Marco Bertoni, ST Microelectronics, Italy
Guido.bertoni@st.com
Joan Daemen, ST Microelectronics, Belgium
Joan.daemen@st.com
Krzysztof Gaj, George Mason University, USA
kgaj@gmu.edu
Tim Güneysu, Ruhr University of Bochum, Germany
guenysu@crypto.rub.de
Anwar Hasan, University of Waterloo, Canada
A.Hasan@ece.uwaterloo.ca
Marc Joye, Technicolor, France, Marc.Joye@technicolor.com
Markus Kuhn, University of Cambridge, UK
Mgk25@cl.cam.ac.uk
Stefan Mangard, Infineon Technologies, Germany
Stefan.Mangard@infineon.com
David Naccache, École Normale Superiéure, France
david.naccache@ens.fr

Elisabeth Oswald, University of Bristol, UK
Elisabeth.Oswald@bristol.ac.uk
Pascal Paillier, Gemalto, France, pascal.paillier@gemalto.com
Francisco Rodríguez Henríquez, CINVESTAV, IPN, Mexico
francisco@cs.cinvestav.mx
Pankaj Rohatgi, Cryptography Research, USA
pankaj.rohatgi@cryptography.com
Kazuo Sakiyama, The University of Electro-Communications, Japan
sakiyama@uec.ac.jp
Erkay Savaş, Sabanci University, Turkey
erkays@sabanciuniv.edu
Patrick Schaumont, Virginia Tech, USA, schaum@vt.edu
Werner Schindler, Bundesamt für Sicherheit in der Informationstechnik, Germany, werner.schindler@cased.de
Sergei Skorobogatov, University of Cambridge, UK
Sergei.Skorobogatov@cl.cam.ac.uk
François-Xavier Standaert, Université Catholique de Louvain, Belgium, fstandae@uclouvain.be
Tsuyoshi Takagi, Kyushu University, Japan, takagi@fun.ac.jp
Pim Tuyls, Intrinsic ID, The Netherlands
pim.tuyls@intrinsic-id.com
Mathias Wagner, NXP Semiconductors, Germany
mathias.wagner@nxp.com

Submission:
Potential authors are invited to upload their manuscript at: http://www.editorialmanager.com/jcen/. Instructions for authors and further information available at the journal homepage: www.springer.com/13389.
For special requests please contact the Editor-in-Chief:
Name: Çetin Kaya Koç,
Address: College of Creative Studies & Department of Computer Science
University of California Santa Barbara
Santa Barbara, CA 93106, USA
Phone: +1 805 893 8565
Email: koc@cs.ucsb.edu