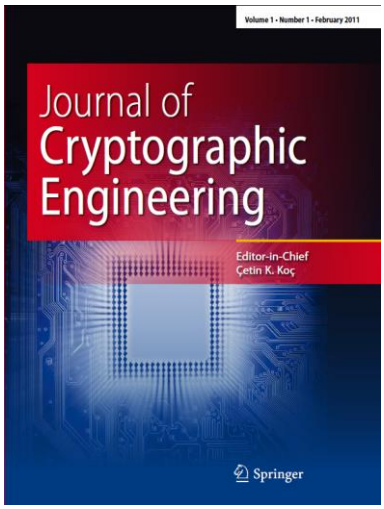
Call for Papers / New Journal Announcement



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. JCEN 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

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

Springer

http://www.springer.com/journal/13389

Journal of Cryptographic Engineering
Editor-in-Chief: Koç, Ç.K.
ISSN: 2190-8508 (print version)
ISSN: 2190-8516 (electronic version)
Journal no. 13389