

Second Advanced Encryption Standard (AES) Candidate Conference

Call for Papers

Rome, Italy; March 22-23, 1999

(updated 2/4/99)

Overview

In August 1998, NIST began Round 1 of technical analysis for the Advanced Encryption Standard (AES) development effort, by announcing fifteen candidate algorithms at the First AES Candidate Conference in Ventura, California. Near the end of Round 1, the Second AES Candidate Conference (AES2) will be held March 22-23, 1999, in Rome, Italy. At this conference, Round 1 technical analysis will be presented and discussed, along with views as to which candidates should be selected as finalists for Round 2.

AES2 will be followed immediately by the Sixth Fast Software Encryption Workshop (FSE6), at the same location.

European coordinator: William Wolfowicz

Paper Submission Requirements

NIST invites people to submit analysis and recommendation papers that address particular AES candidates and/or issues that will directly impact NIST's selection of the five or fewer Round 2 finalists.

To avoid the possible duplication of papers accepted for AES2 and the Fast Software Encryption Workshop 1999 (FSE6), papers will NOT be considered for AES2 if they are identical to papers accepted for FSE6.

Topics

NIST has suggested several areas for comment in the September 14, 1998 Federal Register [FR98]. These include comments on:

- AES Evaluation Criteria listed in the September 12, 1997 Federal Register (*Security, Cost, Algorithm and Implementation Characteristics*),
- Intellectual Property,
- Cross-Cutting Analysis – comparing the entire field of candidates, and
- Overall Recommendations – which candidates should and/or should not be selected for Round 2, with supporting justification.

Format

- Adobe PDF, Postscript, or LaTeX formats (*PDF is preferred*)
- Limit - 15 pages.
- Note that all submitted papers must be in final form – drafts and outlines will not be accepted, due to the short time period between the deadline and the conference.
- Although complete papers are preferred, the Program Committee will review any extended abstracts received, evaluating them against the same criteria used for complete papers. Note that the extended abstract should be as detailed as possible, and it shall be provided in its final form, ready for printing in the AES2 Proceedings. (*added 1/22/99*)

Address

- Paper submitters shall submit a signed "Author's Release" form (see attached), either with the paper itself or by FAX to Jim Foti at (301) 948-1233. (*added 1/22/99*)
- E-mail: AESEFirstRound@nist.gov ; Please send the document either as an attachment or embedded within the message.

- ❑ Regular (postal) mail: Information Technology Laboratory, Attn: AES Candidate Comments, Room 540, NIST, 100 Bureau Drive, STOP 8970, Gaithersburg, MD 20899-8970
- ❑ Courier delivery: Information Technology Laboratory, Attn: AES Candidate Comments, NIST, Building 820, Room 540, Gaithersburg, MD 20899

Note that all papers submitted – whether accepted or not for AES2 - shall become part of the public record as noted in [FR98]. (*modified 1/22/99*)

There will be a rump session at AES2, during which attendees may briefly present items of relative interest. (*added 1/22/99*)

Dates

Paper submission deadline: February 1, 1999
Notification of acceptance: March 1, 1999
Conference: March 22-23, 1999
Round 1 comments, final deadline: April 15, 1999

Program Committee

Miles E. Smid (chair), *NIST*
David Aucsmith, *Intel Corporation*
Thomas Berson, *Anagram Labs*
Craig Clapp, *PictureTel Corp.*
Jim Foti (coordinator for NIST reviewers), *NIST*
Anatoly Lebedev, *LAN Crypto, Inc.*
Susan Langford, *Certicom Security Integration Services (2/4/99)*
William Wolfowicz, *FUB*

Author's Release

I, _____, do hereby grant to the National Institute of Standards and Technology (NIST) the nonexclusive right to reproduce or to have reproduced, prepare or have prepared in derivative form, and distribute or have distributed copies of the attached paper submission for the Second AES Candidate Conference (AES2). This includes, at a minimum, the inclusion of this paper (if accepted) in the AES2 conference proceedings to be distributed to AES2 conference attendees, and the paper's posting on NIST's AES home page at <http://www.nist.gov/aes>.

I am aware that this paper - whether accepted for presentation at AES2 or not - shall become part of the public record, since it is being submitted in response to NIST's Federal Register Notice of September 14, 1998 (Volume 63, Number 177), which solicits comments on the fifteen first round AES candidate algorithms.

Agreed to and Accepted

Signature of Author or Submitter

Date

Printed Name: _____

Title: _____

Organization: _____