Third Advanced Encryption Standard (AES) Candidate Conference

AES3

Call for Papers

13-14 April 2000; New York, New York, USA

Overview

In the summer of 1999, NIST began Round 2 of the technical analysis of five candidate algorithms that have been selected as finalists for the Advanced Encryption Standard (AES) development effort. Near the end of Round 2, the Third AES Candidate Conference (AES3) will be held 13-14 April 2000, at the Hilton New York and Towers, in New York, New York, USA. At AES3, technical analysis from Round 2 will be presented and discussed, along with views as to which of the finalists should be selected as the AES winner(s).

AES3 will follow the Fast Software Encryption Workshop 2000 (FSE2000), which will be held at the same location on 10-12 April 2000.

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 AES winner(s).

To avoid the possible duplication of papers accepted for AES3 and FSE2000, papers will NOT be considered for AES3 if they are identical to papers accepted for FSE2000. Under a separate announcement, the FSE program committee has invited people to submit papers for FSE2000, including papers that discuss the AES finalists. Authors should submit their papers to either AES3 or FSE2000, but not to both. Papers on AES candidates submitted to FSE2000 and rejected will (with the author's permission) automatically be submitted to AES3.

Topics

NIST has suggested several areas for comment in the September 15, 1999 Federal Register notice (FR99). These include comments on:

- Cryptanalysis of the finalists,
- Intellectual Property of the finalists,
- Cross-Cutting Analysis – comparing all five of the finalists for particular characteristics,
- Overall Recommendations: which finalist(s) should and/or should not be selected for the AES, with supporting justification,
- Implementation requirements of the AES FIPS (Federal Information Processing Standard), and
- AES Evaluation Criteria listed in the September 12, 1997 Federal Register notice *(Security, Cost, Algorithm and Implementation Characteristics)*.

These suggestions are described in greater detail in FR99.

Format

- Adobe PDF, Postscript, Rich Text Format (RTF), Microsoft Word (Word97-compatible), or LaTeX formats *(PDF is preferred – please embed all fonts used within the document)*
- Limit 15 pages.
- Note that all submitted papers must be in final draft form – outlines will not be accepted.
- 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 AES3 Proceedings.

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.
- E-mail: AESround2@nist.gov; Please send the document either as an attachment or embedded within the message.
- Address: NIST, Attn: AES Candidate Comments, Building 820 Room 423, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930, USA.

Note that all submitted papers – whether accepted or not for AES3 - shall become part of the public record, since they are being submitted to NIST in response to a call for public comments.

There will be a recent results ("rump") session at AES3, during which attendees may briefly present items of relative interest.

Dates

Paper submission deadline:	January 15, 2000
Notification of acceptance:	March 8, 2000
Final version due for proceedings:	March 15, 2000
AES3 Conference:	April 13-14, 2000
Round 2 comments, final deadline:	May 15, 2000

Program Committee

TBD

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 Third AES Candidate Conference (AES3). This includes, at a minimum, the inclusion of this paper (if accepted) in the AES3 conference proceedings to be distributed to the 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 AES3 or not – shall become part of the public record, since it is being submitted in response to NIST's Federal Register Notice of September 15, 1999 (Volume 64, Number 178), which solicits comments on the five finalist AES candidate algorithms.

Agreed to and Accepted

_____ _____

Signature of Author or Submitter Date

Printed Name: _____

Title: _____

Organization: _____

Title of Paper Submitted: _____