Horst Görtz Institut
für Sicherheit in der Informationstechnik

IAIK TUG

Fourth Conference on the Advanced Encryption Standard (AES)
"AES – State of the Crypto Analysis"

AES4

www.aes4.org

Hilton Hotel Bonn, Germany
10-12 May, 2004

Between August 1998 and April 2000 NIST organized 3 conferences on the Advanced Encryption Standard. In October 2000, the selection of Rijndael as proposed AES was announced. In November 2001, the AES was announced officially in FIPS 197.

The evaluation of the cryptographic strength of Rijndael hasn't stopped after the announcement and official publication of the AES. On the contrary, the increased visibility of the algorithm selected has spurred many interesting new approaches to cryptanalyze (full or reduced versions of) Rijndael.

The Ruhr-University of Bochum organizes the fourth conference on the AES in cooperation with the Graz University of Technology and NIST.

The goal of the conference is to provide an overview of the newest developments related to the cryptographic security of the AES and to bring interested cryptographers together.

Invited Talks:

- Nicolas T. Courtois
  (Axalto Smart Cards)
- Ivo Desmedt
  (Florida State University)
- Jean-Charles Faugere
  (University of Paris VI)
- John Kelsey
  (NIST)
- Vincent Rijmen
  (Graz University of Technology and Cryptomathic)
- Carlos Cid
  (Royal Holloway, University of London)

2nd Call for contributions

Besides several invited talks by various specialists in the field, the program of AES4 contains also slots to be filled in by submitted contributions. The programme committee invites submissions concerning different aspects of the AES cipher (Rijndael).

This includes, but is not limited to:

- cryptographic attacks on full or reduced versions
- observations about the design that may be relevant to the security
- protecting implementations against side-channel attacks
- comparisons with other block ciphers

All submissions will be reviewed.

It is planned to publish the final proceedings in the Springer Lecture Notes in Computer Science series (approval pending).

Instructions for Authors

Authors who wish to present their results are invited to submit a paper of at most 15 pages describing their contribution. The submission should start with a title and a short abstract summarizing the paper. The submission must be **anonymous**, with no author names, affiliations, acknowledgements, or obvious references.

All submissions should be sent by email to sowa@hgi.ruhr-uni-bochum.de. Submissions should be in PostScript, Adobe PDF or Word format.

Important Dates

Submission deadline:	April 21st, 2004
Acceptance notification:	April 30th, 2004
Workshop:	10-12 May, 2004

Mailing List

If you want to receive further information, please subscribe to the mailing list at www.aes4.org.

Program Committee

- Hans Dobbertin (program chair)
  (Horst Görtz Institute, Ruhr-University Bochum)
- Don Coppersmith
  (IBM)
- Lars Knudsen
  (Technical University of Denmark)
- Vincent Rijmen (program chair)
  (Graz University of Technology and Cryptomathic)
- Nicolas T. Courtois
  (Axalto Smart Cards)
- Matt Robshaw
  (Royal Holloway, University of London)

Organizer

Aleksandra Sowa (general chair)

Horst Görtz Institute
Ruhr-University Bochum
Universitätsstr. 150
44780 Bochum
Germany

Phone: +49 (0) 234 – 32 23262
Fax: +49 (0) 234 – 32 14430

sowa@hgi.ruhr-uni-bochum.de

Supporters

CRYPTOMATHIC
e-Security for better business

NIST

Last update: 06.04.2004