Announcement and Call for Papers

Journal of CRYPTOLOGY

The Official Journal of the International Association for Cryptologic Research

Research in cryptology has increased dramatically during the past decade. There are currently several conferences each year devoted entirely to cryptologic research, and several more conferences that regularly accept papers on cryptology. Due to this increased level of research, Springer-Verlag, in cooperation with the International Association for Cryptologic Research, will begin publication of the **JOURNAL OF CRYPTOLOGY.** All aspects of modern cryptologic research will be covered. All papers will be subject to thorough technical review as part of the evaluation process. The first issue of the new journal is expected to appear in early 1988. Publication of three issues per year is planned.

Aims and Scope

JOURNAL OF CRYPTOLOGY will provide a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis will be covered, including information theoretic and complexity theoretic perspectives, as well as implementation, application and standards issues. Illustrative topics include public key and conventional algorithms and their implementations, cryptanalytic attacks, pseudorandom sequences, computational number theory, cryptographic protocols, zero knowledge complexity, untraceability, privacy, authentication, and key management. In addition to full-length technical and survey articles, short notes are acceptable.

Instructions for Authors

JOURNAL OF CRYPTOLOGY is now accepting papers for review for publication, with the first issue scheduled to appear in March 1988. All papers should be submitted in English. They should include an introduction explaining the motivation and background for the work being reported as well as a short but informative abstract. It is an important aim of the journal to achieve a quick turnaround, enabling timely reporting of significant results.

To submit a paper, four copies should be sent to any member of the editorial board.

The title page should include the author's affiliation and mailing address, several key words, and the abstract.

Illustrations should be camera ready and available at the time of notification of acceptance.

Copyright transfer forms will be provided and should be signed and returned immediately.

References should be listed at the end of the article in alphabetical order by authors' last names; this alphabetical list should be numbered consecutively starting with [1]. References should be cited in text by their arabic numeral in brackets. Sample references:

[1] D.E. Denning, Cryptography and Data Security, Addison-Wesley, Menlo Park, CA, 1982.

[2] W. Diffie and M.E. Hellman, New directions in cryptography. IEEE Transactions on Information Theory, Vol. IT-22(6), pp. 644-654 (Nov. 1976).

[3] O. Goldreich, S. Micali, and A. Wigderson, Proofs that yield nothing but their validity and a methodology for cryptographic design. Proceeding of the 27th Annual Symposium of Foundations of Computer Science, 1986, pp. 174-187.

###

Dr. Ernest Brickell
Room 2Q-392
Bell Communications Research
435 South Street
Morristown, NJ 07960

Springer-Verlag/Publishers
New York Incorporated
175 Fifth Avenue
New York, New York 10010