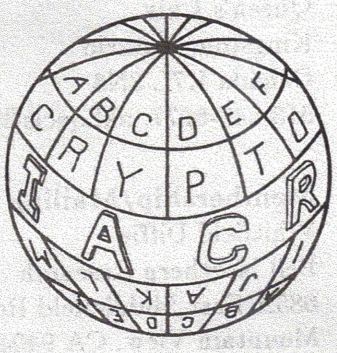
IACR



NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 1 Number 2 July 1984

CONTENTS

IACR Officers and Directors

1984-85 Membership Application Form

International Association for Cryptologic Research

This form must be filled out and returned if you want to be a member of the IACR or a subscriber to the newsletter during 1984-85. Participation in an IACR sponsored conference during 1984 entitles you to become a member or subscriber during 1984-85 without further payment, however, **you must return this form.**

Membership is open to all persons supporting the purpose of IACR, which is to further research in cryptology and related fields. Membership benefits include a subscription to the newsletter, voting privileges, and a membership card (probably a "smart card"). Full-time students may become members at reduced fees provided they obtain a signature certifying their status from a faculty member at their institution.

Name _____

Affiliation/Institution _____

Address _____

_____

_____

Telephone: Work _____ Home _____

Electronic address: Network _____ Address _____

Type of membership desired (check one)

_ Regular member (Dues: $15)
_ Full-time student member (Dues: $5)
Institution _____
Faculty signature _____
_ Newsletter subscription only (Fee: $15)

Check here if you paid the registration fee for

EUROCRYPT 84 _ CRYPTO 84 _

Amount enclosed (U.S.$ payable to IACR) _____
(If you checked one of the conferences above, no fees are owed.)

Return this form to: Robert R. Jueneman, Computer Science Corp.,
6565 Arlington Blvd., Falls Church, VA 22096

Comments from the President

Dorothy E. Denning

First let me congratulate Norbert Cot, General Chair, and Ingemar Ingemarsson, Program Chair, for their superb job organizing and running EUROCRYPT 84. The workshop, which was held in Paris, April 9-11, was a huge success with 170 attendees. A business meeting was held Monday evening to establish policies and procedures for joining the IACR, make preliminary plans for EUROCRYPT 85, consider a possible bylaw revision (decision was made to defer revisions), elect Norbert and Ingemar to the Board of Directors, and perform miscellaneous other business. Some of these items will be discussed in this note along with various other topics.

Membership in IACR

This newsletter contains an application form for joining the IACR. **You must complete and return this form** if you want to remain or become a member. Persons not returning this form will be deleted from the membership mailing list. The membership dues are $15 for regular members and $5 for full-time students, but if you paid the registration fee for EUROCRYPT 84 or CRYPTO 84, no fees are owed. In the future, you will be able to join or renew your membership when you register for EUROCRYPT or CRYPTO, but initially it is necessary to send in the form. Membership benefits include a subscription to the newsletter, voting privileges, a membership card, and reduced fees at conferences (beginning with EUROCRYPT 85). We are hoping to provide "smart cards" for membership cards, and are working with CCETT and Paymatic-Schlumberger in France on this. It is also possible to subscribe to the newsletter without joining the IACR; the fee for this is also $15.

EUROCRYPT 85

For those of you who like to plan ahead, EUROCRYPT 85 will be held in Linz, Austria. The tentative dates are April 9-11, 1985 (same dates as for EUROCRYPT 84). Franz Pichler of the University of Linz has generously agreed to be the General Chair for the meeting.

CRYPTO 84/85

And for those of you who really like to plan ahead, CRYPTO 85 will be held in Santa Barbara, August 18-21, 1985. This is the week after the conference on computational number theory, which will be held in Arcata, northern California (for more information, contact Andrew Odlyzko at AT&T Bell Labs, Murray Hill).

Meanwhile, don't miss CRYPTO 84 in Santa Barbara, August 19-22. The quality and quantity of papers submitted to this conference since its beginning in 1981 has been steadily improving; this year over 50 papers were submitted, from which the program committee chaired by Bob Blakley acceped about 35. The program includes the latest results on breaking iterated knapsacks, factoring, computing discrete logs, authentication and digital signatures, public key cryptography, cryptographic protocols, and many other topics. There will be an IACR business meeting at CRYPTO 84, and all members are invited to attend. For more information, contact Tom Berson, General Chair (address on front cover).

Logo

Since nobody leapt at the opportunity to design a logo for the association, I took on the challenge myself. But I will not assume full blame for the outcome (see cover)! Tom Berson suggested the globe to reflect our international status. Brendt Morris provided the cipher that appears in part on the globe - see if you can figure out the complete cipher. Brendt did not make any claims about the security of the cipher in case a "trapdoor" was found. Ed Ashcroft did the drawing after my feeble attempts completely lacked the proper perspective. Janet Grosser produced the final copy.

EUROCRYPT 84

APRIL 9-11, 1984 LA SORBONNE, 75005 PARIS FRANCE

PROGRAM

MONDAY, APRIL 9, 9:30 a.m. - 1:00 p.m.
Session A1, 9:30 - 11:00 a.m. (Chairwoman: D. Denning).

1. Cryptology and complexity (invited lecture), *G. Ruggiu (Thomson-CSF).*

2. RSA-bits are 0.5 + ε secure, *C.P. Schnorr, W. Alexi (Universität Frankfurt).*

3. On the number of close-and-equal pairs of bits in a string (with implementations on the security of RSA's L.S.B.), *O. Goldreich (MIT).*

4. Design of public-key cryptosystems using idempotent elements, *J.P. Pieprzyk (Technical Academy of Bydgoszcz).*

Session A2, 11:20 a.m. - 1:00 p.m. (Chairman: I. Ingemarsson).

5. A public-key cryptosystem based on rational functions, *R. Nobauer (Klagenfurt Universität).*

6. Permutation polynomials and public-key cryptosystems, *W.B. Müller (Klagenfurt Universität).*

7. Variable - Speed: A new dimension in secure sequence generation, *J.L. Massey, R.A. Rueppel (ETH Zürich).*

8. The stop-and-go generator, *T. Beth (Erlangen Universität), F.C. Piper (Westfield College, University of London).*

9. Pseudo random properties of cascade connections of clock controlled shift registers, *D. Gollman (Linz Universität).*

MONDAY, APRIL 9, 2:20 - 6:00 p.m.
Session B1, 2:20 - 4:00 p.m. (Chairman: C. Schnorr).

10. The quadratic sieve integer factoring algorithm (invited lecture), *C. Pomerance (The University of Georgia).*

11. Factoring algorithms at Sandia National Labs (invited lecture), *G. Simmons (Sandia National Labs.).*

12. Strong primes are easy to find, *J.A. Gordon (Cybermation Ltd).*

13. On using the exclusive-or function as a security amplifier: applications to factoring based encryption and pseudo random

Session B2, 4:40 - 6:00 p.m. (Chairman: J. Massey).

14. On cryptosystems based on polynomials and finite fields, *R. Lidl (University of Tasmania).*

15. The wiretap channel II, *A. Wyner (AT&T Bell Lab).*

16. Equivocation for homophonic ciphers, *A. Sgarro (Università di Trieste).*

17. Propagation characteristics of the DES, *M. Davio, Y. Desmedt, J.J. Quisquater (Philips Research Lab/La. ESAT).*

TUESDAY, APRIL 10, 8:00 - 12:40 a.m.
Session C1, 8:00 - 10:00 a.m. (Chairman: D. Chaum).

18. Time-division multiplexing scramblers: selecting permutations and testing the system, *A. Ecker (Hahn-Meitner-Inst.Berlin).*

19. User functions for the generation and distribution of encipherment keys, *R.W. Jones (International Computers Ltd.).*

20. An optimal class of symmetric key generation systems, *R. Blom (Linköping University).*

21. On the use of the binary multiplying channel in a private communication system, *B. Smeets (University of Lund).*

22. Secrecy and privacy in a local area network environment, *G.B. Agnew (ETH Zürich).*

23. Subliminal channel, *G.J. Simmons (Sandia National Labs).*

Session C2, 10:40 - 12:40 a.m. (Chairman: T. Beth).

24. Cryptography and medicine, *M.F. Lechat (Ecole de Santé Publique, Bruxelles).*

25. Security on the British telecom satstream service, *C.B. Brookson (British Telecom. Research Lab.).*

26. An encryption and authentification procedure for tele-surveillance systems, *W. Wolfowicz, O. Brugia, S. Improta (Fondazione Ugo Bordoni).*

~~27~~. Cryptographic aspects of software protection, *R.M.F. Goodman (University of Hull).*

28. A method of software protection based on the use of smart cards and cryptographic techniques, *I. Schaumueller (Voest-Alpine AG, Linz), E. Piller (Honeywell Bull AG, Vienne).*

29. Estimation of some encryption functions implemented into smart cards, *H. Groscot (Université Paris 6).*

TUESDAY, APRIL 10, 2:15 - 7:00 p.m.

Invited session on smart cards (President: A. Turbat, Chairman: J. Goutay).

Session D1, 2:15 - 3:45 p.m.

30. Introductory remarks, *A. Turbat (DGT, Délégation carte à mémoire).*

31. The smart card, key for Data security, *R. Moreno (Innovatron).*

32. Smart card applications in security and Data protection, *J. Goutay (Infoscript).*

33. The CP8 smart card and cryptology, *Y. Girardot (Bull CP8).*

34. The smart card as a solution to key management in networks, *C. Bedier (Thomson).*

35. Payment security at P.O.S. based on smart cards and cryptology, *C. Guion (Flonic-Schlumberger).*

36. Smart cards and conditional access, *L. Guillou (CCETT).*

Session D3, 5:45 - 7:00 p.m.

37. Panel discussion on security and smart cards: Present and Future *(with A. Turbat, R. Moreno, J. Goutay, Y. Girardot, C. Bedier, C. Guion, L. Guillou and P. Lemarchand (Philips Data System).*

WEDNESDAY, APRIL 11, 9 a.m. - 1:00 p.m.

Session E1, 9:00 - 10:40 a.m. (Chairman: J. Gordon).

38. An overview of discrete logarithms (invited lecture), *A. Odlyzko (AT&T Bell Labs).*

39. A secure protocol for the oblivous transfer, *C. Rackoff (University of Toronto), S. Micali (MIT), M.J. Fischer (Yale University).*

40. On concurrent identification protocols, *O. Goldreich (MIT).*

Session E2, 11:00 - 12:40 a.m. (Chairman: J.J. Quisquater).

41. File authentification. A rule for constructing algorithms, *H. Block (SAKdata AB).*

42. A digital seal function based on error correcting codes, *P. Godlewski (ENST, Paris).*

43. Fast Cryptanalysis of the Matsumoto-Imai Public key scheme, *Y. Desmedt & al. (Katholieke Universität Leuven).*

44. The dinning cryptographers problems: unconditional sender anonymity, *D. Chaum (University of California, Santa Barbara).*

45. Trees of unlinkeable pseudonyms traversable by digitally signed credentials, *D. Chaum (University of California, Santa Barbara).*

WEDNESDAY, APRIL 11, 2:20 - 4:40 p.m. (Chairman: W. Diffie).

Session F1, 2:20 - 3:20 p.m.

46. An overview of custom VLSI implementations of the RSA cryptosystem (invited lecture), *R. Rivest (MIT).*

Session F2, 3:40 - 4:40 p.m.

47. On finite state machine classification of crypto-analytic attacks, *F. Pichler (Linz Universität).*

48. Non-commutative, non-linear functions for data integrity, *S. Harari (Université de Toulon et du Var).*

49. Nonlinear functions and their applications in cryptography, *J.P. Pieprzyk (Technical Academy of Bydgoszcz).*

Symposium On Security And Privacy

The 1984 Symposium On Security And Privacy sponsored by the IEEE Technical Committee On Security And Privacy was held at the Claremont Hotel in Oakland, California, from April 30 to May 2, 1984. The following papers were presented at the Symposium during a session devoted to Cryptology and chaired by G. Robert Blakely of Texas A & M University.

1) A Secure One-Way Function Built from DES
   Robert Winternitz, Stanford University

2) Searching for Public-Key Cryptosystems
   Neal Wagner, Drexel University

3) A New Paradigm for Individuals in the Information Age
   David Chaum, U.C. Santa Barbara

SESSION ON SECURE COMMUNICATIONS AT THE TWELFTH BIENNIAL SYMPOSIUM ON COMMUNICATIONS

A session entitled "Secure Communications" was held at the Twelfth Biennial Symposium on Communications which was held at Queen's University in Kingston, Ontario, Canada, on June 4-6, 1984. The Symposium is jointly sponsored by the Department of Electrical Engineering at Queen's and the Department of Communications (Federal Government of Canada).

The session was chaired by Dr. G. H. MacEwen of the Department of Computing and Information Science at Queen's and there were three papers in the session which may be of interest to readers of the IACR Newsletter. The titles and authors of the relevant papers are:

(i) "Specification of a Distributed Multi-Level Secure System: The Lucid/Dataflow Approach", J. I. Glasgow and G. H. MacEwen, (Queen's University).

(ii) "A Fast Pseudo Random Permutation Generator with Applications to Cryptography", S. G. Akl and H. Meijer, (Queen's University).

(iii) "Sequence Complexity as a Test for Cryptographic Systems", A. K. Leung and S. E. Tavares, (Queen's University).

The Proceedings of the conference have been published (300 pages) and is available from S. E. Tavares, Department of Electrical Engineering, Queen's University, Kingston, Ontario, K7L 3N6, Canada, at $10. (U.S.) per copy.

CRYPTO '84 AUGUST 19-22, 1984

TO BE HELD AT

THE UNIVERSITY OF CALIFORNIA
AT SANTA BARBARA

SPONSORED BY

THE INTERNATIONAL ASSOCIATION
FOR CRYPTOLOGIC RESEARCH

ALL PERSONS INTERESTED IN THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES ARE INVITED AND ENCOURAGED TO ATTEND CRYPTO '84.

ORGANIZING COMMITTEE:

- THOMAS A. BERSON (SYTEK, INC.).....GENERAL CHAIRMAN
- G.R. BLAKLEY (TEXAS A&M).....PROGRAM CHAIRMAN
- JOE TARDO (DIGITAL EQUIPMENT CORP.).....SHOW & TELL
- RICHARD A. KEMMERER (U.C.S.B.).....LOCAL ARRANGEMENTS
- HENRY BEKER (RACAL RESEARCH).....PROGRAM
- DOROTHY DENNING (SRI INTERNATIONAL).....PROGRAM
- RON RIVEST (MIT).....PROGRAM
- MILES SMIDT (NATIONAL BUREAU OF STANDARDS).....PROGRAM
- KAY G. WHITE (SYTEK, INC.).....REGISTRAR

CALL FOR PAPERS

PAPERS ARE SOLICITED ON ALL TOPICS RELATED TO CURRENT WORK IN THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. WE WOULD ALSO LIKE TO INCLUDE A FEW HIGH-QUALITY HISTORICAL PAPERS. PLAN TO SEND SIX COPIES OF YOUR ABSTRACT OR COMPLETE PAPER TO: **PROF. G.R. BLAKLEY, PROGRAM CHAIRMAN,** CRYPTO '84 - DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TEXAS 77843-3368 - PHONE NO. (409) 845-7939 OR 854-3913. DEADLINE FOR PAPERS IS MAY 21, 1984. AUTHORS WILL BE NOTIFIED BY JULY 1, 1984. INFORMAL QUERIES AS TO THE SUITABILITY OF YOUR TOPIC SHOULD BE DIRECTED TO THE PROGRAM CHAIRMAN.

NEW THIS YEAR

WE WILL PROVIDE AN OPPORTUNITY FOR CRYPTO '84 ATTENDEES TO SHOW AND EXPLAIN TO ONE ANOTHER CRYPTOGRAPHIC ITEMS OF CURRENT OR HISTORICAL INTEREST. IF YOU HAVE SOMETHING WHICH YOU COULD BRING TO CRYPTO '84, PLEASE CONTACT **JOE TARDO, SHOW & TELL CHAIRMAN,** CRYPTO '84 - DIGITAL EQUIPMENT CORPORATION, TWO/C11, 1925 ANDOVER STREET, TEWKSBURY, MD 01876. PHONE: (617) 858-3014.

REGISTRATION

CAMPUS ACCOMMODATIONS WILL BE AVAILABLE FOR ATTENDEES WHO REGISTER BY JULY 16, 1984. THE CHARGES FOR ROOM AND BOARD COVER ALL MEALS FROM DINNER SUNDAY THROUGH LUNCH ON WEDNESDAY, INCLUDING A BEACH BARBECUE TUESDAY EVENING. (ADDITIONAL BARBECUE TICKETS MAY BE PURCHASED FOR $15 EACH.) THE WORKSHOP FEE INCLUDES COCKTAIL PARTIES ON SUNDAY AND MONDAY EVENINGS.

ATTENDANCE IS LIMITED AND EARLY REGISTRATION IS NECESSARY. THE ATTACHED REGISTRATION FORM, TOGETHER WITH **PAYMENT IN FULL** OF THE WORKSHOP FEE AND ROOM AND BOARD CHARGES, IF DESIRED, MUST BE RETURNED **BEFORE JULY 15, 1984.**

GENERAL INFORMATION

FOR GENERAL QUESTIONS REGARDING CRYPTO '84, PLEASE CONTACT **THOMAS A. BERSON, GENERAL CHAIRMAN** - SYTEK, INC., 1225 CHARLESTON ROAD, MT. VIEW, CA 94043 - (415) 966-7300.

CRYPTO '84

PROGRAM

PKC AND SIGNATURES

H.C. Williams	Some Public-Key Crypto-Functions as Intractable as Factorization
Benny Chor, Ronald L. Rivest	A Knapsack Type Public Key Cryptosystem Based on Finite Fields Arithmetic
Adi Shamir	Identity-Based Cryptosystems & Signature Schemes
H. Ong, C.P. Schnorr, A. Shamir	Efficient Signature Schemes Based on Polynomial Equations
Neal R. Wagner	Searching for Public-Key Cryptosystems
Taher El Gamal	A Public Key Cryptosystem & a Signature Scheme Based on Discrete Logarithms
S.C. Serpell, C.B. Brookson, B.L. Clark	A Prototype Encryption System Using Public Key

RANDOMNESS AND ITS CONCOMITANTS

S.C. Kothari	On a Generalized Threshold Scheme
Oded Goldreich, Shafi Goldwasser, Silvio Micali	On the Cryptographic Applications of Random Functions
Manuel Blum, Shafi Goldwasser	An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information
Umish V. Vazirani,	Efficient & Secure Pseudo-Random

Selim G. Akl, Henk Meijer	A Fast Pseudo Random Permutation Generator With Applications to Cryptology
R.C. Fairfield, R.L. Mortenson, K.B. Coulthart	A LSI Random Number Generator (RNG)
G.R. Blakley, Catherine Meadows	Relativized Security of Ramp Schemes

PROTOCOLS AND AUTHENTICATION

Tom Tedrick	Fair Exchange of Secrets
David Chaum	New Secret Codes Can Prevent a Computerized Big Brother
H.J. Beker	Proposal for: Secure Key Management & Authentication
Mordechai Yung	Cryptoprotocols: Subscription to a Public Key, The Secret Blocking & the Multi-Player Mental Poker Game
Gustavus J. Simmons	Authentication Theory/Coding Theory
Steven Fortune, Michael Merritt	Poker Protocols
D.W. Davies, D.O. Clayden	A Message Authenticator Algorithm Suitable for a Main Frame Computer

ANALYSIS AND CRYPTANALYSIS

Alan G. Konheim	Cryptanalysis of ADFGVX Encipherment Systems
G.R. Blakley	Cryptography without the Finiteness Assumption
Marc Davio, Yvo Desmedt, Jean-Jacques Quisquater	Dependence of Output on Input in DES: Small Avalanche Characteristics

Benny Chor, Oded Goldreich	RSA/Rabin Least Significant Bits are $\frac{1}{2} + \frac{1}{\text{poly}(\log N)}$ Secure
Ernest F. Brickell	New Results on Cryptanalyzing Iterated Knapsacks
George B. Purdy	The Weaknesses of Multiple Use Discrete-Log Key Exchange
J.A. Reeds, J.L. Manferdelli	DES Has No Per Round Linear Factors

CRYPTOSYSTEMS AND OTHER HARD PROBLEMS

S. Chen	On Rotation Group and Encryption of Analog Signals
Marc Davio, Yvo Desmedt, Jozef Goubert	Efficient Hardware & Software Implementations for the DES
J.A. Davis, D.B. Holdridge	An Update on Factorization at Sandia National Laboratories
R.C. Mullin, S.A. Vanstone	The Computation of Logarithms in $GF(2^n)$
Norman Proctor	A Self-Synchronizing Cascaded Cipher System With Dynamic Control of Error Propagation
Albert C. Leighton, Stephen M. Matyas	The History of Book Ciphers
R.C. Fairfield, A. Matusevich, J. Plany	A LSI Digital Encryption Processor (DEP)
Burton S. Kaliski, Jr.	Wyner's Speech Scrambler

CRYPTO '84 REGISTRATION FORM

TO BE HELD AT

THE UNIVERSITY OF CALIFORNIA
AT SANTA BARBARA
AUGUST 19-22, 1984

SPONSORED BY

THE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

☐ MALE
☐ FEMALE

NAME _____
(PLEASE TYPE OR PRINT CLEARLY)

AFFILIATION/INSTITUTION _____

ADDRESS _____

_____

_____

TELEPHONE ( ) _____ ALTERNATE PHONE ( ) _____

WORKSHOP FEE: ☐ REGULAR ($100) ☐ FULL-TIME STUDENT ($70)

ROOM & BOARD:
☐ SINGLE ROOM ($120)
☐ DOUBLE ROOM ($100/PERSON)
☐ NOT REQUIRED
☐ PREFERRED ROOMMATE, IF APPLICABLE _____

ROOMS ARE IN THE UNIVERSITY DORMATORIES. PRICE INCLUDES TICKET FOR TUESDAY BARBECUE.

☐ ADDITIONAL BARBECUE TICKETS: _____ AT $15.00.

TOTAL AMOUNT ENCLOSED: _____

PLEASE MAKE CHECK PAYABLE TO "CRYPTO '84".

EXPECTED DATE AND APPROXIMATE TIME OF ARRIVAL, IF KNOWN: _____

MAIL THIS REGISTRATION FORM AND YOUR CHECK TO:
CRYPTO '84 - REGISTRATION
KAY G. WHITE
C/O SYTEK, INC.
1225 CHARLESTON ROAD
MOUNTAIN VIEW, CA 94043 U.S.A.

"COMPUTER SECURITY– A GLOBAL CHALLENGE"

IFIP/SEC'84

Second International Congress and Exhibition on Computer Security
Toronto, Ontario, Canada
September 10-12,1984

CALL FOR PAPERS

Sponsored by IFIP

Organized by CIPS

IFIP

The International Federation for Information Processing was formed in Paris in 1960 by the representatives of eight national computer associations, that had worked together with UNESCO in preparation for the first World Computer Congress held there the previous year. As of January 1st, 1984 44 national organizations representing 49 countries are members of IFIP.

At the IFIP Congress held in Paris, France during September 1983, an IFIP Technical Committee on Computer Security (TC 11) was established. The major aims of the committee are:

- to establish a frame of reference for security common to both EDP professionals and the public
- to exchange experience of practical security work
- to evalute data processing techniques from security viewpoints
- to inform on new protective techniques and their proper use
- to promote security as being an important integral part of data processing

Call for papers

IFIP's Second International Congress on Computer Security will be held in Toronto, Canada on September 10-12, 1984. This is a followup to the successful Congress held in May 1983 in Sweden. The Congress is being organized by the Canadian Information Processing Society (CIPS).

The Congress objectives are:

- to promote the discipline of computer security as a profession
- to provide an international forum for the practical and theoretical aspects of computer security
- to address all the differing interests of auditors, management, security practitioners, and the data processing community

Contributions are solicited describing practical experience and research in computer security. Some suggested topic areas are:

- Communications and network protection
- Cryptographic protection
- Disaster recovery
- EDP audit
- Facilities protection
- Identification/Authentication
- Modeling secure systems
- Policy and organization
- Quality assurance
- Risk management
- Security awareness & education
- Security software
- Systems architecture for security
- Transborder dataflow

Instructions for authors

Papers must be written and presented in English and be typed clearly, double spaced, on one side of each sheet.

Two copies of each paper are to be submitted to the Congress Secretariat.

Each copy should contain the following items:

a) Title of the paper

b) Name, country, affiliation, and full mailing address and telephone number of the author(s).

c) An abstract 200 to 400 words in length, typewritten in English.

d) All illustrations, with titles, numbered consecutively and properly related to the text.

e) All papers must show the author's name in the upper left-hand corner and should be numbered consecutively in the upper right-hand corner.

The authors shall give an estimate of the time required for their presentation (presentations to be between 30 to 45 minutes).

Authors should submit two complete copies of their papers to the Congress Secretariat to arrive by February 29, 1984.

Notice of acceptance will be mailed to the authors by April 30,1984 and a preliminary Congress Program will be published shortly thereafter

Authors of accepted papers will be required to produce the text of the final paper in a form suitable for reproduction in the Congress Proceedings according to the instructions to be provided. The final paper must be submitted to the Congress Secretariat before May 31,1984.

Deadlines

Feb. 29	Two copies of the paper required in the Secretariat's hands.
Apr. 30	Authors notified of their acceptance.
	Preliminary Congress Program published.
May 31	Authors of accepted papers are required to submit copies of their paper for inclusion in the Congress Proceedings.
Sep. 10	CONGRESS

All correspondance should be addressed to the Congress Secretariat at:

IFIP/SEC'84
International Security Congress 1984 Inc.
160 Duncan Mill Road
Don Mills, Ontario
Canada
M3B 1Z5

Telephone: 416-447-1821

Congress Organization

Program Committee

Jerome Lobel, Chairman
Honeywell Information Systems
Phoenix, Arizona, U.S.A.

Organizing Committee

Carol Lipsett, Chairman
Canadian Imperial Bank of Commerce
Toronto, Ontario, Canada

IFIP/SEC'84

SECOND INTERNATIONAL CONGRESS AND EXHIBITION ON COMPUTER SECURITY
TORONTO, ONTARIO, CANADA, SEPT. 10-12, 1984

Yes, I wish to: ☐ Submit a paper ☐ Exhibit at the Congress ☐ Register for the Congress

Name _____

Organization _____

Complete address _____

_____

_____

_____

Telephone _____

PLEASE MAIL TO IFIP/SEC'84, INTERNATIONAL SECURITY CONGRESS 1984 INC.
160 DUNCAN MILL ROAD, DON MILLS, ONTARIO, CANADA, M3B 1Z5

Call For Papers

1984 IEEE Symposium on Foundations of Computer Science

The 25th Annual IEEE Symposium on Foundations of Computer Science, sponsored by the Computer Society's Technical Committee on Mathematical Foundations of Computing, will be held on Singer Island, off West Palm Beach, Florida, on October 24-26, 1984. Papers presenting original research on theoretical aspects of computer science are being sought.

Suggested Topics: Typical, but not exclusive, include:

- Algorithms and Data Structures
- Computability and Complexity Theory
- Cryptography
- Theory of Data Bases
- Logic of Programs
- Theory of Formal Languages and Automata
- Theory of Logical Design, Layout and VLSI
- Models of Computation
- Semantics of Programming Languages
- Parallel and Distributed Computation

Submission of papers: Authors should send ten copies of a detailed abstract (*not* a full paper) by May 7, 1984 to the Program Committee Chairman:

Professor Richard M. Karp
Computer Science Division
573 Evans Hall
University of California
Berkeley CA 94720

Authors will be notified of acceptance or rejection by June 25, 1984. A copy of each accepted paper, typed on special forms for inclusion in the symposium proceedings, will be due by August 13, 1984.

IMPORTANT

Because of a large number of submissions is anticipated, authors are advised to prepare their detailed abstracts carefully. It is recommended that each submission begin with a succinct statement of the problem, a statement of the main results and an explanation of the significance that is suitable for a general research audience. Technical development of the work, directed to the specialist, should follow as appropriate. In any case, the entire extended abstract, with comparison to extant work, should not exceed 2500 words (ten typed double-spaced pages). Submissions departing significantly from these guidelines risk rejection without consideration of their merits.

Meeting Format: The format of the meeting, including time allocations for presentations, will be determined by the Program Committee. Authors having a preference for a short (10-15 minute) or long (20-30 minute) presentation should express it at the time of submission. Such a preference will not influence acceptance, and time allocation will not be noted in the proceedings or affect the space allocation for the paper. If submissions warrant, the committee will compose a program of parallel sessions.

Machtey Award for Best Student Paper: This award, of up to $400 to help defray expenses for attending the Symposium, will be given for that paper which the Program Committee adjudges the most outstanding paper written solely by a student or students. To be considered for the award, an abstract must be accompanied by a letter identifying all authors as full-time students at the time of submission. (At its discretion, the Committee may decline to make the award or may split the award among two or more papers.)

Symposium Committees

Program Committee

Shimon Even
Leo J. Guibas
Richard M. Karp
Dexter Kozen
Michael O'Donnell
Larry Stockmeyer
Ivan H. Sudborough
Martin Tompa
Leslie G. Valiant
Mibalis Yannakakis

LOCAL ARRANGEMENTS
Frederick Hoffman
Department of Mathematics
Florida Atlantic University
Boca Raton, FL