IACR

NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 6 Number 1 January 1989

CONTENTS

IACR Contact List

IACR Business Office
P.O. Box 303
Palo Alto, CA 94302-0303
USA

Officers . . .

President
Thomas A. Berson
Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94301
USA
+1 415 324 0100, berson@kl.sri.com

Secretary-Treasurer
Wyn L. Price
National Physical Laboratory
Teddington, Middx TW11 0LW
United Kingdom
+44 1 977 3222

Eurocrypt 89 Chair
Joos Vanderwalle
ESAT Katholieke Universiteit Leuven
Kard. Mercierlaan
B-3030 Heverlee
Belgium
+32 16 22 09 31
eurocrypt@kulesat.uucp

Crypto 89 Chair
Kevin McCurley
IBM Research K53/802
650 Harry Road
San Jose, CA 95102-6099
USA
+1 408 927 1708, mccurley@ibm.com

Newsletter Editor
Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
+1 519 885 1211 x3041
gbagnew@ccng.waterloo.edu

J. of Cryptology Editor
Ernest Brickell
Div. 1423
Sandia National Laboratories
Albuquerque, NM 87185
USA
+1 505 846 1546
efbrick@sandia-2.arpa

Directors . . .

Henry Beker
Zergo Limited
Millbank House
High Street
Hartley Wintley, Hants RG27 8PE
United Kingdom
+44 25126 4545

Thomas A. Berson
(see President)

Thomas Beth
Institut fur Informatik
Universitaet Karlsruhe
Postfache 6380
D-7500 Karlsruhe 1
Fed Rep Germany
+49 721 608 4205
beth@iravcl.germany.csnet

Ernest Brickel
(see J. of Cryptology Editor)

David Chaum
C.W.I.
Box 4079
1009 AB Amsterdam
The Netherlands
+31 20 529 4167
chaum@mcvax.cwi.nl

Norbert Cot
E.H.E. Informatique
45 rue des Saints-Peres
F-75 006 Paris
France
+33 1 47 03 31 27

Dorothy E. Denning
Digital Equipment Corp.
Systems Research Center
130 Lytton Ave.
Palo Alto, CA 94301
USA
+1 415 853 2252

Whitfield Diffie
Bell Northern Research
685A E. Middlefield Rd.
Mountain View, CA 94039-7277
USA
+1 415 940 2513
wd@ai.su.edu

John Gordon
Cybermation Ltd.
Ashley Ho., Ashley Rd.
St. Albans, Herts AL1 5JR
United Kingdom
+44 727 40151

Ingemar Ingemarsson
Linkoping University
Dept. of Electrical Engineering
S-581 83 Linkoping
Sweden
+46 13 281 300

David Kahn
Cryptologia Magazine
120 Wolley's Lane
Great Neck, NY 11023
USA
+1 516 487 7181

Stephen Kent
Bolt Beranek and Newman
10 Moulton Street
Cambridge, MA 02238
USA
+1 617 873 3988
kent@bbn.com

Ronald Rivest
MIT Lab for Computer Science
545 Technology Square
Cambridge, MA 02139
USA
+1 617 253 5880
rivest@mc.lcs.mit.edu

Editor's Corner

Happy New Year and may 1989 be a happy and prosperous year! In reflection, 1988 was also a good year for the IACR. The first two issues of the Journal of Cryptology have appeared this year. Both EUROCRYPT'88 and CRYPTO'88 were very successful and attracted more attendees than the previous year. (Speaking of CRYPTO'88, Hal Fredericksen is to be congratulated for the excellent organization and smooth running of CRYPTO'88 - thanks Hal.) Plans were also begun for conferences in Japan and Australia (1989 and 1990 respectively). All in all, a good year.

There have also been some changes in the IACR executive. As you may know, Jim Massey has stepped down as President. I'm sure I speak for all the members of the IACR in thanking Jim for the excellent job and for all his time and patience in performing the many thankless tasks required of the president. We also welcome our new president, Thomas Berson (former Secretary/Treasurer) and our new Secretary/Treasurer Wyn Price to their posts.

Changes are also in the works for the IACR. Tom has outlined some of these in the President's Message on the next page.

So as we say good-bye to 1988, we look forward to even more exciting events in 1989.

Check your mailing label!
If is says "Exp 12/88" you must RENEW NOW.
Use the form inside the back cover.

From The President . . .

1988 was a year of tremendous growth for IACR. In January we had 375 members. By December we had doubled to about 750. The growth is certainly gratifying. It comes, I believe, from the high quality of our conferences and publications. Since the last issue of the *Newsletter* was published we have held Crypto 88 and published Vol. 1 Number 2 of the *Journal of Cryptology*.

You will find a report on Crypto 88 elsewhere in this *Newsletter*. IACR thanks Hal Fredricksen and his crew for organizing the conference. We also thanks Shafi Goldwasser, who put the program together with the help of Eric Bach, Paul Barrett, Gilles Brassard, Oded Goldreich, Andrew Odlyzko, Charles Rackoff, and Ron Rivest. Of course the conference couldn't have happened without the authors and attendees.

During 1988 IACR launched the *Journal of Cryptology*, edited by Ernie Brickell and published and distributed by Springer Verlag. Two of the three numbers of Volume 1 have been published and number three is now being assembled. If you are an associate editor, a referee or an author please help us lubricate the Journal's pipeline. Ernie reports that Volume 2 is shaping up nicely. Springer reports that, in addition to IACR members, the *Journal of Cryptology* is now taken by over one hundred libraries.

Our regular series of conferences will continue. Eurocrypt 89 will be held at Houthalen, Belgium. It is being organized by Joos Vanderwalle and Jean-Jaques Quisquater. Crypto 89 will be held in Santa Barbara. It is being organized by Kevin McCurley and Gilles Brassard. Peter Landrock is organizing Eurocrypt 90 to be held in Aarhus, Denmark. I expect Crypto 90 to be held in Santa Barbara. Please send me your (self-)nominations for General Chairman of Crypto 90.

Beyond these regularly scheduled conferences, IACR is co-sponsoring two others. Auscrypt will be held in Sydney, Australia in January 1990. Jennifer Seberry is organizing Auscrypt and will be shortly sending information to all members. Asiacrypt 91 is being co-sponsored with the Japanese ISEC organization. It is expected to be held near Tokyo in November 1991.

All of these activities are put on entirely by volunteers from our professional community. They work without recompense and often with very little thanks. We need more workers. Won't you become active in IACR? If your answer is "yes" write me a letter or telephone me.

As you might expect, the rapid growth in membership and the increasing complexity of our program has strained our administrative systems. I will be working during my term as President to move IACR in the direction toward being run more professionally. (It simply is no longer possible to keep track of all our members using files organized in a shoebox.)

I have organized a business office for IACR, and have been trying to hire a part-time secretariat to keep track of our affairs. We're at that awkward stage, where we are too big to do without a secretariat and too small to require one full-time. The work of the secretariat requires office skills, computer literacy, intelligence, common sense, and attention to detail. Most people who have these qualifications are already happily employed. After several false starts, I have turned temporarily to one of the best workers I know, my wife, Dorothy Berson. She would dearly love to be put out of the job. Any takers?

Tom Berson

Crypto '88 Conference

The annual Crypto conference, eighth in the series, sponsored by the International Association for Cryptologic Research, Inc. (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California at Santa Barbara, was held in Santa Barbara, California on August 21-25, 1988. Some 220 participants, from 23 countries, heard 34 papers presented in a single stream, with a rump session of 23 papers. Attendees came from universities, government agencies and commercial organizations.

The general chairman of the conference was Professor Hal Fredricksen, of the Naval Postgraduate School, Monterey, CA, and the programme chairperson was Professor Shafi Goldwasser, of MIT, assisted by an international committee. The call for papers had solicited original papers on all theoretical as well as practical aspects of cryptography. About half of the offered papers were accepted for presentation.

The conference sessions covered foundations, zero-knowledge, number theory, cryptographic systems, pseudorandomness, signatures and authentication, theory of cryptographic systems, protocols, security concerns, cryptanalytic techniques, and systems. Three invited papers come from Professor Eric Bach, University of Wisconsin, on "Intractable Problems in Number Theory", Professor Charles Rackoff, University of Toronto, on "A Basic Theory of Public and Private cryptosystems", and Professor Leonard Adelman, University of Southern California, on "The Theory of Computer Viruses". It was notable that many of the papers, submitted as well as invited, related to aspects of zero-knowledge or oblivious transfer protocols, reflecting the considerable interest that this subject has aroused in recent years. Many of the presentations were theoretical in nature, though some addressed practical applications. Proceedings of Crypto '88 will be published by Springer Verlag of Heidelberg, West Germany [in the Lecture Notes in Computer Science series].

At the Crypto '88 meeting Dr Thomas Berson of Anagram Laboratories, Palo Alto, CA, succeeded Professor James Massey, of ETH, Zurich, Switzerland, as President of IACR. Dr Wyn Price, of National Physical Laboratory, UK, succeeded Dr Berson as Secretary/Treasurer of IACR.

The Crypto conferences, held each August in California, alternate with the Eurocrypt conferences held under the sponsorship of IACR at different sites in Europe. The 1988 Eurocrypt conference, held at Davos, Switzerland, in May, attracted even more attendees than did Crypto.

1988 has seen the emergence of the *Journal of Cryptology*, the official journal of IACR; the Editor-in-Chief is Dr Ernest Brickell of Sandia Laboratories, and the publishers are Springer International. The coverage of this journal will be similar to that of the Crypto and Eurocrypt conferences, but the papers published will, of course, be more substantial. It is a main goal of the *Journal* to provide a forum for the publication of important new results and surveys in all areas of cryptography and cryptanalysis.

Wyn L. Price, Secretary/Treasurer

EUROCRYPT '89

April 10–13, 1989
Houthalen, BELGIUM

A WORKSHOP ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES

sponsored by the
International Association for Cryptologic Research (IACR)

Organizing Committee
Joos Vandewalle *(General chairman)*
Tri An Banh *(ULg, Liège)*
Marijke De Soete *(RUG, Gent)*
Jean Doyen *(ULB, Bruxelles)*
Jean-Marie Goethals *(UCL, Louvain-la-Neuve)*
René Govaerts *(KUL, Leuven)*
Emile Peeters *(CEC, Brussels)*
Jean Ramaekers *(FUN, Namur)*
Bart Preneel *(Local arrangement)*

Program committee
Jean-Jacques Quisquater *(Program chairman)*
Paul Camion *(INRIA, Rocquencourt)*
Yvo Desmedt *(UW, Milwaukee)*
Louis Guillou *(CCETT, Rennes)*
Johan Håstad *(RIT, Stockholm)*
Llorenç Huguet *(UAB, Barcelona)*
Wyn Price *(NPL, Teddington)*
Rainer Rueppel *(Crypto AG, Steinhausen)*
Johan van Tilburg *(PTT-DNL, Leidschendam)*

SUBJECT

The conference deals with all aspects of the theory and the application of cryptography including symmetric and asymmetric ciphers, authentication, protocols, secure transactions, signatures, sequences and linear complexity, hardware and software topics, security of telecommunication systems and computer networks. The program includes a rump session and a session on open problems. The proceedings of the workshop will be published by Springer Verlag in the *Lecture Notes in Computer Science* series.

LOCATION

The meeting will be held in the calm, spacious and relaxing atmosphere of the Conference Centre Hengelhoef, 80 km east of Brussels and Antwerp (address : Domein Hengelhoef, Hengelhoefdreef 1, B–3530 Houthalen–Helchteren, telephone +32–11–38 01 16, telex 39 345 hengel). The Centre is situated in the heart of Limburg, in the midst of a large park with woods and ponds. It offers a wide range of sports accomodations. Further details about tourist information will be mailed with the confirmation of your registration.

ACCOMODATIONS

Conference attendees and accompanying persons will be accomodated in 200 studio-apartments grouped around the congress building. These studio-apartments are completely equipped, a sitting-room, a kitchenette, toilet and shower, a private terrace, and sleeping facilities with one or two beds. The price for a single/double room and breakfast will be 4,000/3,000 Bfr. (1 US$ $\simeq$ 37 Bfr). Reservations can be extended before and after the conference.

TRANSPORTATION

Houthalen is only 80 kilometers away from Brussels airport. A bus service will be provided just before and after the conference. It is also possible to take the train via Brussels to Hasselt. The Centre is served by a bus service from Hasselt. Finally, if you are arriving by car, the Centre is near to the exit 30 *"Park Midden Limburg"* of the E 314 freeway. Further details will be provided with the confirmation of your registration.

CONFERENCE EVENTS

The conference starts on Monday, April 10th with lunch and ends on Thursday, April 13th early afternoon. Social activities, including a reception, a rump session and a banquet are planned for the evenings. A short visit to the Bokrijk open air museum is scheduled on Monday late afternoon. There will be an IACR Business meeting on Thursday morning.

CLIMATE

Although the weather during April can be cool, (10 – 15°*C*) with a good chance on rain, sunny — and warmer- – days are quite likely.

REGISTRATION *Deadline : March 15, 1989*

The workshop fee is 12,000 Bfr. This fee includes four lunches, coffee breaks, the Monday evening aperitif and dinner, Tuesday evening rump session and dinner, Wednesday evening banquet and the dues to the *International Association for Cryptologic Research* (IACR). These later dues entitle you to become a member of the IACR for 1990 without any additional payment and to receive the IACR's *Journal of Cryptology*, published by Springer Verlag, free of charges during thatyear. The workshop fee must be paid upon registration, which should be performed before March 15, 1989. There will be no registration at the door.

A reduced workshop fee of 8,000 Bfr. is offered to full time students, undergraduate or graduate, if their registration form is accompanied by a certification of their student status.

The fee for accompanying persons is 10,500/9,500 Bfr. for a single/double room. It includes Room and Board and all social activities (visit, banquet, ...).

Crypto '89
Call for Papers

The Ninth Annual CRYPTO Conference sponsored by the International Association for Cryptologic Research (IACR) in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California, Santa Barbara, will be held on the campus of the University of California, Santa Barbara, on August 20-24, 1989. Original research papers and technical expository talks are solicited on all practical and theoretical aspects of cryptology. It is anticipated that some talks may also be presented by special invitation of the Program Committee.

Instructions for authors: Authors are requested to send ten copies of a detailed abstract (not a full paper) by March 17, 1989, to the Program Chairperson at the address given below. Abstracts should contain sufficient detail, as well as references to and comparisons with relevant extant work, to enable Program Committee members to appreciate their merits. It is recommended that abstracts start with a succinct statement of the problem and discussion of its significance and relevance to cryptology, appropriate for a non-specialist reader. In order to facilitate blind refereeing, the names of authors and their affiliations should only appear on the cover page of the paper; it should be possible to remove this page and send the papers to Program Committee members. Limits of 10 double-spaced pages and 2500 words (not counting the bibliography and the cover page) are placed on all abstracts. If the authors believe that more details are essential to substantiate the main claims of the paper, they are asked to include a clearly marked appendix that will be read at the discretion of the Program Committee. Abstracts that significantly deviate from these guidelines risk rejection without consideration of their merits. Abstracts received after the March 17 deadline will not be considered, unless they are postmarked not later than March 13 and arrive a reasonable time thereafter. Authors will be informed of acceptance or rejection in a letter mailed not later than May 26.

A compilation of all abstracts accepted will be available at the conference. Authors of accepted papers will be given until July 14, 1989 to submit revised abstracts for this compilation. Complete conference proceedings will be published in Springer-Verlag's Lecture Notes in Computer Science series at a later date. The Program Committee will consider abstracts that have also been submitted to other conferences. However, if a submission is accepted for presentation at more than one conference, the authors may present the results more than once but may publish them in at most one proceedings.

The Program Committee consists of Josh Benaloh (University of Toronto), Russell Brand (Special session chairperson, Lawrence Livermore Laboratory), Gilles Brassard (Committee chairperson, Université de Montréal), Claude Crépeau (Massachusetts Institute of Technology), Whitfield Diffie (Bell Northern Research), Joan Feigenbaum (AT&T Bell Laboratories), James Massey (ETH Zentrum, Zurich), Jim Omura (Cylink Corporation), Gustavus Simmons (Sandia National Laboratories), and Scott Vanstone (University of Waterloo).

Send abstracts to the program chairperson:
Gilles Brassard, Crypto '89
Département IRO
Université de Montréal
C.P. 6128, Succursale "A"
Montréal (Québec)
CANADA H3C 3J7
telephone: (514) 343-6807
email: brassard@iro.umontreal.ca

Other information, contact the general chair:
Kevin McCurley
IBM Research, K53/802
650 Harry Road
San Jose CA 95120–6099
U.S.A.
telephone: (408) 927-1708
Internet: mccurley@ibm.com
Bitnet: mccurley@almvma.

HELP!!!

The editor (that's me) is soliciting suggestions for a new and improved image for the newsletter. Since the newsletter is intended to reflect the interests of the membership, it seems appropriate that the members of the IACR should be invited to contribute. This may take the form of historical notes, new developments, reports on conferences, reports on development of standards impacting the cryptographic community, new product reports (sorry, no commercial advertising), encrypted jokes (clean ones only), or anything you feel may be of interest to your fellow members. Please take the time to support your association.

All contributions can be sent to:

G. B. Agnew
Dept. of Electrical Engineering
University of Waterloo,
Waterloo, Ontario, Canada
N2L 3G1
email: gbagnew@ccng.waterloo.edu

1989 Membership Application (Memberships Expire 12/89)

International Association for Cryptologic Research

Membership is open to all persons supporting the purpose of IACR, which is to further research in cryptology and related fields. Membership benefits include subscriptions to the Journal of Cryptology and to the IACR Newsletter and voting privileges.

Membership is for a calendar year. Persons who attended Eurocrypt 88 or Crypto 88 are already enrolled for the calendar year 1989. Payment on this form will bring Volume 2 (1989) of the Journal of Cryptology.

Full-time students may become members at reduced fees provided they obtain a signature certifying their status from a faculty member at their institution.

Please type or print clearly!

First Name _____ Last Name _____

Affiliation/Institution_____

Address _____

_____

_____

Telephone _____

Network Address_____

Type of membership desired (check one)
__ Regular member (Dues: $40)
__ Full-time Student member (Dues: $20)

Faculty name _____

Faculty signature _____

New Member? ___. Renewing Member? ___.

Amount enclosed (**US$ on a US bank** payable to IACR) $_____

Return this form to: IACR
P.O. Box 303
Palo Alto, CA 94302-0303
USA

IACR
P.O. Box 303
Palo Alto, CA 94302-0303
USA

MENLO PARK CALIF. FEB 17'89 U.S.POSTAGE ≈0.35≈ P.B. METER 6626213

AIR MAIL
PRINTED MATTER

KEVIN MCCURLEY EXP 12/89
IBM ALMADEN RESEARCH K-53
650 HARRY RD
SAN JOSE CA 95120
USA

FIRST CLASS MAIL