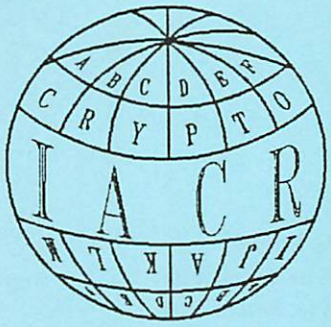


IACR

NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 9 Number 1 January 1992

CONTENTS

IACR Contact List

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

Officers . . .

President - See Election results

Vice President - See Election results

Secretary - See Election results

Treasurer - See Election results

Eurocrypt 92 Chair
Tibor Nemetz
Math. Inst. of the Hungarian
Acad. of Sci.
P.O. Box 127/H-1364
Budapest, Hungary
h1137nem@ella.hu

Crypto 92 Chair
Spyros Magliveras
Comp. Sci. Dept.
Univ. of Nebraska - Lincoln
Lincoln, NE 68588-0115
USA.
402-472-5005
spyros@helios.unl.edu

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
Gilles Brassard
Dept. IRO
Universite de Montreal
C.P. 6128, Succ. "A"
Montreal, Quebec, Canada
H3C 3J7

Directors . . .

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

Ernest Brickel
Sandia National Labs Div 1423
Albuquerque, NM 87185
USA
+1 505 846 7564, efbrick@sandia.gov

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

Whitfield Diffie
Sun Microsystems, MTV01-40
2550 Garcia Ave.,
Mountain View, CA 94043
USA

John Gordon
Lynfield House
Datchworth Green, Herts. 8G3 6TL
United Kingdom
+44 438 811015

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

Jennifer Seberry
Centre for Comm. & Info. Sci.
RM W13, Nebraska Hall,
Univ. of Nebraska, Lincoln Nebraska
USA, 68588-0115

Yvo Desmedt
Dept. of Elec. Eng. & Comp. Sci.
Univ. of Wisconsin - Milwaukee
P.O. Box 784, Milwaukee, WI
USA 53201

See election results for
our three new directors

Editor's Corner

As we start 1992, it seems appropriate to reflect on the events of 1991. The year started under the threat of hostilities in the middle east. Our fears turned to reality as war broke out in January. This almost caused the cancelation of EUROCRYPT'91. Once again, we should thank the general chair, Andy Clark and his organizing committee for their heroic efforts in making EUROCRYPT'91 a resounding success.

Thanks are also due to Burt Kaliski (General Chair) and Joan Feigenbaum (Program Chair) for organizing another great CRYPTO! (worth the conference fee just for the cocktail parties.)

We also sponsored our first (of many) ASIACRYPT in Fujiyoshida this year. Word has it that, the Chair (Shigeo Tsujii), the program co-chairs (Hideki Imai and Ron Rivest) and their committees are to be congratulated for putting on a great conference (I wish I had gone!).

I would also like to welcome all of the new members or the IACR who joined at the conferences this year. Once again, it seems we are growing.

1991 was also a year of changes. This year was an election year and a new group of Officers and three Directors will takeover for 1992. One significant change will be President's position. As you know, Thomas Berson decided not to run again for President of the IACR (he is running as a director). I'm sure every member shares my appreciation to Thomas for all the time and devotion he has given to the IACR both as Secretary-Treasurer and as President over the past few years.

Rainer Rueppel has also decided to step down as Secretary. Again, our thanks are due for all the time and effort Rainer has put into the IACR.

Looking ahead, 1992 will also hold some firsts. Our new President will begin his/her term in 1992. In the face of a changing Europe, it seems appropriate that EUROCRYPT'92 will be held in Hungary. We will again have three IACR affiliated conferences with AUSCRYPT'92 (Gold Coast, Australia).

So, let's bid a fond farewell to 1991, and look forward to the events of 1992.

HAVE A HAPPY AND PROSPEROUS 1992

GBA.

(P.S. I've kept you in suspense long enough, the election results are on the next page...)

ELECTION RESULTS

This is the report of the chief returning officer, Jennifer Seberry.
I declare the following persons elected to be office bearers of the IACR
President: Peter Landrock (123 votes - Vanstone 118 votes -Informal 19 votes)
Vice President: Ingemar Ingemarsson (142 votes -Clark 101-Informal 17)
Treasurer: Kevin McCurley
Secretary: Sherry McMahan
Directors: Tom Berson (153)
Andrew Clark (126)
Hideki Imai (100)
(Moti Yung received 88 votes, Peter Landrock and Ingemar Ingemarrson were removed from the ballot for Director by reason of having already been declared elected for higher office.)
Signed: Jennifer Seberry, Returning Officer, IACR

Report on the Journal of Cryptology

Dear Journal of Cryptology reader and contributor,
Although nothing has really been resolved in the labour dispute between the Canadian Postal Union and the Canadian Government, which is why I have delayed so long this message, mail has been flowing normally* in Canada for more than a month. Therefore, it appears to be perfectly safe to submit your papers directly to me by airmail at my usual address.
I wish to thank Joan Feigenbaum for agreeing to serve as buffer during the postal strike.
In case you wonder, the Journal is doing very well. Assuming that Springer is true to their word, nothing at this point can prevent Volume 5 (the first volume for which I am responsible) from appearing exactly on schedule in 1992. (Precisely, 11 February, 11 June and 8 October are the publication dates; please allow more time for postal delivery.) Whether or not Volume 6, 1993 appears also on schedule is in OUR hands: the editor-in-chief can do nothing without the authors! Although I have no worry for Volume 6 at the current submission rate, more submissions would not hurt.
Editorially yours,

- Gilles Brassard
Editor-in-Chief

* Of course, "normally" means sluggishly when the Canadian Postal "service" is concerned!

MINUTES OF THE IACR BOARD OF DIRECTORS MEETING

At 2:00 p.m. on 11 August, 1991, the meeting of Board of Directors of the International Association for Cryptologic Research was called to order by Tom Berson, President. The Directors present were:

Tom Berson, Norbert Cot, David Chaum, Jennifer Seberry, Gilles Brassard, Whitfield Diffie, Kevin McCurley, Burt Kaliski, Scott Vanstone, Ernie Brickell and Gordon Agnew. Also present were Joan Feigenbaum, Program Chair for Crypto '91, and Sherry McMahan, acting as secretary in Rainer's absence.

The agenda was modified to include under item 13) Other Business, the negotiations with Springer and the use of the mailing list by Whitfield Diffie.

1) Apologies for absence - Apologies were made for Rainer Rueppel, Tom Beth, Andy Clark, Ingemar Ingemarsson, John Gordon and Ron Rivest. Tom Beth had given his proxy to Sherry McMahan and Andy Clark had given his proxy to Tom Berson.

2) Approve Minutes of the Last Meeting - Minutes of the Board meeting held on April 7, 1991 in Brighton had been sent to all the directors. All corrections are to be given directly to Rainer.

3) President's Report - Tom Berson reported that there are no big problems facing IACR at this time. All looks good.

4) Financial Report - Kevin McCurley reported on the interest income earned; the substantial surplus returned to IACR from Eurocrypt '91; that he had moved money from savings to short term CD's in order to earn more interest; and that he had received an inquiry from the IRS and had responded (nothing out of the ordinary). Kevin recommended that there not be an increase of the annual dues for the membership in IACR. Anyone interested in a copy of the tax return should contact Kevin.

5) Plan for Elections - The upcoming elections are for the following positions: three directors (outgoing directors are Tom Beth, Ernie Brickell and Norbert Cot), president, vice president, secretary and treasurer. Individuals who have expressed interest in standing for office are: Andy Clark and Sherry McMahan both for the position of secretary.

Tom read from the ByLaws the guidelines for the election. It was noted that the Bylaws do not address the issue of spoiled ballots. David Chaum, Gordon Agnew and Jennifer Seberry volunteered for the nominating committee. The ballots will be addressed to Jennifer Seberry (at the University of Nebraska) and will be mailed by 1 November. The election will close on 31 December (postmark). Anyone can nominate himself and the nominating committee will also solicit candidates. The nomination will close on 1 October. (Anyone wishing to have a copy of the Bylaws should contact the IACR office.)

6) IACR Logo - the proposed designs were discussed and it was decided that one of the designs would be developed further. David Chaum and Tom Berson will each contact an artist to further develop one of the designs (see attachment A). It was decided by a vote of 7 yes and 1 no, that the artists would be paid $1000 each to develop a logo and logo type in postscript. These two designs would be sent to the Directors by 1 February, 1992 and the logo will be decided at the Board of Directors meeting at Eurocrypt '92.

7) Journal of Cryptology - Gilles Brassard presented his report (see attached two page report.) Gilles presented his nominations for the Editorial Board and the Board of Directors approved unanimously these individuals. Gilles had a meeting with Springer in New York and Springer suggested that the Editors recommend papers to the Editor in Chief. The Editor in Chief will make the final decision on what papers are chosen. Gilles will send a letter to the Editors and will have a meeting this week with those in attendance at Crypto '91.

Discussion followed on the paper review cycle delay in certain areas versus those in other areas. Timeliness of the journal is the major concern with IACR members and Springer.

Scott Vanstone, who served as Program Chair for Crypto '90, said that the camera ready copy of the Proceedings for Crypto '90 was sent to Springer on 2 January, 1991 and that the editor set on it for three months. This has delayed the publishing of the Proceedings until the end of September. Joan Feigenbaum said that she submitted a copy of the Pre-proceedings for Crypto '91 to Springer in hopes that this will help speed up the process for the publishing of the Crypto '91 proceedings.

A discussion followed on how to advertise the Journal and also how to solicit papers for the Journal. Gilles has asked each editor to solicit papers. It was suggested

that Springer have a booth displaying books on cryptography or related topics and past proceedings at crypto conferences. In the past Springer has been invited and did have a display at Eurocrypt '88 in Davos, Switzerland. Scott suggested that IACR contact former members concerning their possible interest in the journal.

8) Multiple Submission Policy Report - Ron Rivest had sent a letter (see attached one page letter). Moti Yung had raised this issue and Joan agreed to give a copy of Ron's letter to Moti.

9) Program Chair Guidelines - Motion carried to accept the Guidelines. The Guidelines will be updated as needed. Please contact Sherry McMahan for a copy of the guidelines.

10) Conferences:

a) Eurocrypt '91 - Thanks to Andy for a great job. Please see attached 4 page report by Andy Clark.

b) Crypto '91 - Burt Kaliski reported that there were 228 registered with 177 on campus (10 accompanying guests) and 55 off campus. Of the 228, 59 had attended Eurocrypt and there were 33 students. Twenty seven countries are represented with 40% from the U.S. Burt had suggestions for future conferences and will pass those to Kevin to be incorporated in the General Chair Guidelines. Joan said that there is a 15 page limit on the papers for the proceedings. Thanks to Burt and Joan for a well organized conference.

c) Crypto '92 - Will be held at UCSB from 16 to 20 August, 1992 with Spyros Magliveras as General Chair and Ernie Brickell as Program Chair.

d) AsiaCrypt '91 - To be held at Fujiyoshida, Yamanashi, Japan from 11 to 14 November, 1991. Kenji Koyama is the General Chair and Hideki Imai and Ron Rivest are Co Program Chair.

e) Eurocrypt '92 - To be held at Hotel Fured, Balatonfured, Hungary. Tibor Nemetz is the General Chair and Rainer Rueppel is the Program Chair. See attached 2 page report from Tibor.

f) Auscrypt '92 - To be held at the Gold Coast, Queensland, Australia from 14 to 17 December, 1992. Bill Caelli is General Chair and Jennifer Seberry is Program Chair.

11) ICSU Affiliation - Norbert Cot visited with ICSU in Paris and reported that ICSU is a 100 years old, non governmental organization. The goal of ICSU is to promote science throughout the world. There are three types of members: a) national body (fee $1000); b) Science Unions (fee 2.5% of annual income); and c) Associates (fee $500). Three reasons to join ICSU are a) for the interdisciplinary programs; b) for the research programs; and c) to gain from ICSU's lobbying power. After Norbert's report questions were asked about ICSU's charter and what happens if ICSU and IACR do not agree on a specific issue. Norbert will get a copy of ICSU's charter and send along with the above information to the Board before Eurocrypt '92. A decision whether to join or not will be made when the Board meets at Eurocrypt '92.

12) Possible merger with TC on Security and Privacy - TC on Security and Privacy has approached IACR about a possible merger. Much discussion followed and it was decided that Jennifer and Whit would meet with IEEE and report back to the Board.

13) Other Business -

a) Negotiations with Springer - Tom reported that there has been no major progress with the negotiations of the new contract with Springer. Tom will meet with individuals of the Board at lunch on Monday, 12 August to discuss the topics that should be raised by him when he meets again with Springer.

b) Whit Diffie has changed jobs and is now with Sun Microsystems. Whit asked if he could use freely or for a fee the IACR mailing list to do a mailing of a notification of his move. It was decided by the Board that the mailing list is for use only by IACR and it was not in the direct interest of IACR to set a precedence and allow the mailing list to be used in this way.

14) IACR Assembly Planning - The IACR Business Meeting will be held on Wednesday evening at the end of the day's talks. During the meeting Tom will introduce the directors, Kevin will give the financial report, Gilles will speak about the Journal, Burt and Joan will say a few words about Crypto '91, Tom will present the schedule of IACR sponsored crypto conferences for the next few years and then the floor will be given over to the membership for questions and discussions.

Meeting was adjourned at approximately 5:45 p.m.

Respectfully submitted,

Sherry S. McMahan

Enclosures:
Logo design A
Report by Gilles Brassard on the Journal of Cryptology
Letter from Ron Rivest on Multiple Submission Policy
Eurocrypt '91 report by Andy Clark
Eurocrypt '92 report by Tibor Nemetz

A Report on CRYPTO '91
August 11-15, 1991 - Santa Barbara, CA

CRYPTO'91 continued the history of relaxing yet stimulating late-summer southern-California workshops on cryptography with 227 participants from 26 countries. Academia and industry were equally represented with about 45 percent of the participants, and the remaining 10 percent were from government. There were 32 students.
The United States topped the list of participants by country, but this year no country had a majority. There was even a participant from the Soviet Union. The country breakdown was as follows:

Australia	4	Germany	14	Spain	1
Austria	1	Israel	3	Sweden	1
Belgium	5	Italy	5	Switzerland	4
Brazil	1	Japan	13	Taiwan	2
Canada	21	Korea	6	The Netherlands	3
China	3	Norway	7	United Kingdom	9
Denmark	6	Singapore	1	United States	91
Finland	2	South Africa	3	Yugoslavia	1
France	19	Soviet Union	1		

The conference featured 39 lectures including three that were invited by the program committee. Whit Diffie made a fine effort in coordinating about half that number of lectures during the Rump Session. The program committee had the difficult task of determining the best of many submissions, and their commitment is appreciated.
Acknowledgement is due to:
Joan Feigenbaum, Program Chair (AT&T Bell Laboratories, USA)
Tom Berson (Anagram Laboratories, USA)
Ingemar Ingemarsson (University of Linkoping, Sweden)
Ueli Maurer (Princeton University, USA)
Kevin McCurley (Sandia National Laboratories, USA)
Michael Merritt (AT&T Bell Laboratories, USA)
Moni Naor (IBM Almaden, USA)
Eiji Okamoto (NEC, Japan)
Josef Pieprzyk (University of New South Wales, Australia)
Tony Rosati (Newbridge Microsystems, Canada)
Moti Yung (IBM Yorktown, USA)
The organizing committee put in extra hours to process all the registrations and learned quite a bit about international finances in the process. They also selected artwork, pasted up the abstract book, and answered phone calls and electronic mail. My thanks go to:
Jeff Fassett (RSADSI, USA)
Ginny Kirkley (RSADSI, USA)
Kellie Risso (RSADSI, USA)
Kurt Stammberger (RSADSI, USA)
Jimmy Upton (Comtech Labs, USA)

Kit Boettcher and her staff at UCSB supervised local arrangements behind the scenes efficiently. The conference was highlighted by a last-minute replacement of the traditional Goleta Beach barbecue with a catered dinner in De la Guerra Commons accompanied by a woodwind quintet from Music Academy of the West. Apparently it was the first time in almost 10 years that CRYPTO's barbecue had been rained out.

The budget for CRYPTO'91 was about $90,000, and it appears that income and expenses will balance almost exactly.

CRYPTO '91 was sponsored by the International Association for Cryptologic Research, 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. Additional support from RSA Data Security is gratefully acknowledged.

It was a pleasure to serve the IACR as general chair of CRYPTO'91. I look forward to further work with my fellow cryptographers.

Burt Kaliski
General Chair, CRYPTO '91
December 1991

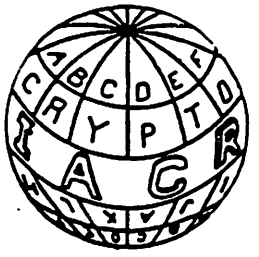
"Peace I leave with you; my peace I give to you." (John 14:27)

Report on ASIACRYPT'91

ASIACRYPT'91 was held at the Hotel Highland Resort, Fujiyoshida, Japan on November 11-14, 1991. This is the first international symposium on cryptology held in Asia. The symposium was co-sponsored by the IACR and the Institute of Electronics, Information, and Communication Engineers of Japan and had 188 attendees from 16 different countries. The general chairman was Prof. S. Tsujii from the Tokyo Institute of Technology. The program co-chairmen were Prof. R.L. Rivest from Massachusetts Institute of Technology and Prof. H. Imai from Yokohama National University. them arrived too late and were rejected without reviewing. The other 97 papers were reviewed by 14 members of the program committee and 39 were accepted for presentation in 8 technical sessions. In addition to them the symposium program included four special sessions for invited lectures. The guest speakers were Dr. D.W. Davies from U.K., Prof. M. Rhee from Hanyang University, Prof. J. Mizusawa from University of Tokyo, and Prof. Rivest. There was also a rump session, where 12 papers were read.

As the Hotel Highland Resort is located at the foot of Mt.Fuji and the weather was fine throughout the symposium, the participants enjoyed the beautiful view of the famous mountain as well as hot discussions in each session.

Hideki Imai



CONFERENCE ANNOUNCEMENT

EUROCRYPT '92

May 24–28, 1992
Hotel Füred, Balatonfüred, Hungary

A Workshop on the Theory and Applications of Cryptographic Techniques

Sponsored by the International Association for Cryptologic Research (IACR).

EUROCRYPT 'NN constitute a series of European conferences dedicated to the theory and applications of cryptographic techniques. **EUROCRYPT '92** will be held between 24-28 May 1992, at Hotel Füred in Balatonfüred, Hungary.

The *scientific programme* deals with all aspects of cryptography. (Please, turn over for a Call for Papers.) It is planned to start on Monday, 25 May. In order to be present at the beginnings, you are invited to arrive on Sunday, 24 May.

The *conference site*, Balatonfüred is located at the northern shore of the largest lake in Central Europe: Lake Balaton. The town has been famous for its medical springs for centuries. It is about 120 km away to the west from the capital and easily accessable by car from all European countries. Bus service from the Budapest Airport terminals will be provided at a reasonable frequency and price.
Hotel Füred lies on the beach of the lake, which is not yet owercrowded at the time of the conference but the wether is already of early summer. Tennis court and other sport facilities are at the quests' disposal.

Predicted hotel prices (for your orientation, only):
A double bed room costs 75.OO US$/night, the same with single occupancy 65.00 US$.
Apartment for two is 105.00 US$/night, with extra 10.00 US$ for extra bed.

Predicted registration fee: 360.00 US$, including the Proceedings of the conference.
Accompanying persons (lunches, receptions, banquet): 120.00 US$

Our *appointed travel agent*, **Malév Air Tours** will conduct all the social arrangements offering pre- and post conference tours, sight seeings.

Please, return the enclosed *registration form* even if your chance to attend the conference is very low. Thus you will ensure receiving any updated information of Eurocrypt '92. You may expect our 2^{nd} Announcement from 20 January, 1992.

The members of the Hungarian Organizing Committee,
László Babai, György Biró, Ferenc Ledniczky, László Lovász, Edit Omaisz, István Vajda
and the General Chair, Tibor Nemetz
are looking forward to greeting you in the conference.

Correspondence to the local OrgComm. should be addressed to:
Tibor Nemetz, Math. Inst. of the Hungarian Acad. of Sci.
P.O.Box. 127/ H-1364 Budapest, Hungary
Courier address: Budapest V., Reáltanoda 13–15
E-mail: h1137nem@ella.hu
Fax: (36-1)-117-71-66

CALL for PAPERS

EUROCRYPT '92

May 24–28, 1992

Hotel Füred, Balatonfüred, Hungary

A Workshop on the Theory and Applications of Cryptographic Techniques

Sponsored by the International Association for Cryptologic Research (IACR).

Original papers are solicited on all aspects of cryptography including symmetric and asymmetric ciphers, authentication, cryptanalysis, protocols, secure transactions, signatures, sequences and linear complexity, hardware and software topics, security of telecommunication systems and computer networks.

Send 10 copies of an extended abstract of at most 10 double-spaced pages to the Programme Chair (address below).

The abstract should clearly indicate the results achieved, their significance, and their relation to other work in the area.

To facilitate blind refereeing, authors are asked to supply a separate cover page indicating title and author, and start the next page with title and abstract of the paper.

The deadline for submissions to the conference will be 15th January 1992.

Submissions that deviate significantly from these guidelines risk rejection without consideration of their merits.

Authors will be notified about acceptance or rejection of their papers by 27th March '92.

A compilation of all accepted abstracts will be available at the conference.

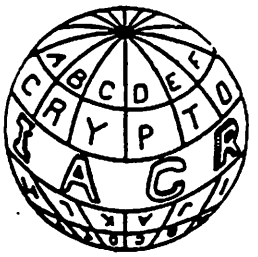
Proceedings from the conference are planned to be published in Springer Verlag Lecture Notes in Computer Sciences.

Programme Chair:
Dr. Rainer A. Rueppel
R^3 Security Engineering
Bahnhofstraße 242
CH–8623 Wetzikon
Switzerland
Tel: +41–1-930 53 58
Fax: +41–1-930 74 28
E-mail: rueppel@nimbus.ethz.ch

General Chair:
Dr. Tibor Nemetz
Math. Inst. of the HAS
P.O. Box 127
H–1364 Budapest
Hungary
+36–1-117 71 75
+36–1-117 71 66
h1137nem@ella.hu

Programme Committee Members:

Kevin McCurley, Sandia National Labs, USA; Yvo Desmedt, Univ. of Wisconsin, USA; Joan Feigenbaum, AT&T Bell Labs, USA; Jovan Golic, Univ. of Belgrade, Yugoslavia; Tor Helleseth, Univ. of Bergen, Norway; Peter Landrock, Aarhus Univ., Denmark; Tatsuaki Okamoto, NTT Labs, Japan; Jennifer Seberry, Univ. of NSW, Australia; Othmar Staffelbach, GRETAG, Switzerland; Jacques Stern, ENS–DMI, France; Istvan Vajda, Technical Univ. of Budapest, Hungary.



EUROCRYPT '92

May 24-28, 1992

Hotel Füred, Balatonfüred, Hungary

REGISTRATION FORM

Please, return this registration form if you wish to receive updated information about Eurocrypt'92. The next Announcement will be distributed from 15th January 1992.

We ask you to assist our scanner by filling in the blocks in capital letters or in typing.

First /given/ mane/s/:

Name (family name):

Address (including country and postal code):

Return to: Tibor Nemetz, General Chair, Eurocrypt'92
Math. Inst. of the Hungarian Acad. of Sci.
P.O.Box. 127/ H-1364 Budapest, Hungary
Fax: (361)-117-71-66

CRYPTO '92

Call for Papers

The Twelfth 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 16-20, 1992. 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 **12 copies** of a detailed abstract (not a full paper) by April 27, 1992, to the Program Chair at the address given below. Submissions must arrive on time or be postmarked no later than April 22, 1992 and sent by airmail in order to receive consideration by the Program Committee. It is required that submissions start with a succinct statement of the problem addressed, the solution proposed, and its significance to cryptology, appropriate for a non-specialist reader. Technical development directed to the specialist should follow as needed.

Abstracts that have been submitted to other conferences that have proceedings are **not** eligible for submission to Crypto.

Crypto **submissions must be anonymous.** This means that names and affiliations of authors should only appear on the title page of the submission; it should be possible to remove this page and send the papers to Program Committee members. A Latex style file that produces output in this format is available by email from the Program Chair. A limit of 10 pages of 12pt type (not counting the bibliography or the title page) is placed on all submissions.

Authors will be informed of acceptance or rejection in a letter mailed on or before June 17, 1992. A compilation of all accepted abstracts will be available at the conference. Authors of accepted abstracts will be given until July 20, 1992 to submit revised versions 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 consists of Ernie Brickell (Chair, Sandia National Laboratories), Ivan Damgard (Aarhus University, Denmark), Oded Goldreich (Technion, Israel), Burt Kaliski (RSA Data Security), Joe Kilian (NEC), Neal Koblitz (University of Washington), Ueli Maurer (ETH, Switzerland), Chris Mitchell (Royal Holloway, England), Kazuo Ohta (NTT, Japan), Steven Rudich (Carnegie Mellon), Yacov Yacobi (Bellcore).

Send submissions to the Program Chair:
Ernest F. Brickell, Crypto '92
Division 1423
Sandia National Laboratories
Albuquerque, NM 87185 USA
Telephone: (505)-845-7655
Fax: (505)-845-7442
Internet: efbrick@cs.sandia.gov

For other information, contact the General Chair:
Spyros S. Magliveras, Crypto '92
Dept. of Computer Science and Engineering
University of Nebraska - Lincoln
Lincoln, NE 68588-0115
Telephone: (402)-472-5005
Fax: (402)-472-7767
Internet: spyros@helios.unl.edu

AUSCRYPT'92

DECEMBER 14 - 17, 1992

CONFERENCE ANNOUNCEMENT

Auscrypt'92 is the second workshop and conference on **cryptology** to be held in Australia. The conference is to be held in association with the **International Association for Cryptologic Research (IACR)** in cooperation with the Information Security Research Centre (ISRC) and the School of Mathematics at the Queensland University of Technology (QUT). The conference will commence on Monday 14th December 1992 at **Somerset College**, a private secondary college located near to the **Gold Coast** region of Queensland, Australia.

SOMERSET COLLEGE

Somerset College is a private secondary college situated in a rural setting at Mudgeeraba on the Gold Coast in the South-East region of Queensland, Australia. The college is a few minutes drive from the beaches of the Gold Coast as well as being near to the hinterland rain-forests and mountain area. The Gold Coast is Australia's premier tourist centre with a number of major theme parks, such as **SeaWorld, DreamWorld, MovieWorld** as well as a number of Australian wild-life parks. Somerset College is well placed to make the conference a success with a broad range of academic facilities, a library, computer laboratories and related services.

CLIMATE

In early December, the Gold Coast will be quite warm with temperatures ranging from around 20 degrees C overnight to up to 32 degrees during the day.

ACCOMMODATION

As Australia's premier tourist area, the Gold Coast offers a broad range of accommodation ranging from small. low-cost motels to five-star international grade hotels and resorts. The Gold Coast also houses **Jupiter's Casino** and its associated hotel complex.

ORGANISING AND PROGRAMME COMMITTEES

Overall Conference Chair:	Professor Bill Caelli, QUT
Programme Chair:	Professor Jennifer Seberry, University of New South Wales

FURTHER INFORMATION

For further information on the conference please contact the general chairman for the conference as follows:

Professor William J. Caelli
General Chair - Auscrypt'92
Information Security Research Centre
Queensland University of Technology
GPO Box 2434
BRISBANE QLD 4001
AUSTRALIA

Phone:	+61 - 7 - 864 2752
Facsimile:	+61 - 7 - 221 2384
e-mail:	w.caelli@qut.edu.au

CRYPTOGRAPHIC PROTECTION OF MEMBERSHIP LISTS*

JOAN FEIGENBAUM†, ERIC GROSSE† AND JAMES A. REEDS†

Abstract. We present a simple algorithm for encrypting membership lists. The encrypted lists and search software can be distributed to members of the organization, who can use them to make legitimate queries. However, it is difficult to use the encrypted list for unauthorized purposes, such as the generation of sales lists. We illustrate the method by applying it to the SIAM membership list, yielding a package that can be widely distributed.

1. Introduction. Professional societies have long faced the question of what to do with their membership lists. There are clearly good reasons to give copies of the list to all members of the society: Communication among the members serves the goals of the profession and fosters a sense of camaraderie among the members. On the other hand, if numerous copies of the membership list are in circulation, some are bound to fall into the hands of insurance salesman, senders of junk mail, rival societies, etc. This dilemma is, of course, faced by many organizations besides professional societies and is exacerbated by the existence of computerized lists.

We propose to ameliorate the problem by cryptography. Given a membership list L, our method produces an encrypted list L' and a lookup program P' with the following properties.

- For any query key q, $P'(q, L') = \{ v \in L \mid q \text{ matches } v \}$.
- Given L' and P', it is difficult to reconstruct L.

This is a special case of the *database protection problem.* That is, the databases in question are simply a collection of records with explicit search keys. A more complicated special case, that of automaton-structured linguistic databases, is considered in [FLW89].

2. Algorithm. The starting point for our algorithm is a standard table-encryption technique first developed by Needham (see Denning's book [D82, Section 3.6] for a thorough discussion).

Let L be a set of (*key,value*) pairs $\{ (k_i, v_i) \mid 1 \leq i \leq n \}$ where k_i come from some set K of syntactically valid keys. Construct a corresponding L' and an access program P' as follows.

Choose a one-way hash function h whose domain is K. Ideally, such a function h would be polynomial-time computable, mapping from K into integers 1 through M with the property that, given $1 \leq j \leq M$, it is computationally infeasible to find $h^{-1}(j) \subset K$. For a more thorough discussion of one-way hash functions, refer to [M89, NY89].

Let *Enc* and *Dec* be encryption and decryption functions such that $Dec(Enc(x, y), y) = x$ for all x and y. An encrypted list L' is derived from L as follows: For every (k, v) pair in L, a pair $(h(k), Enc(v, k))$ is inserted into L'. The lookup program P' can be as simple as

---

* Typeset on October 18, 1991.

† AT&T Bell Laboratories, Murray Hill NJ 07974 USA.

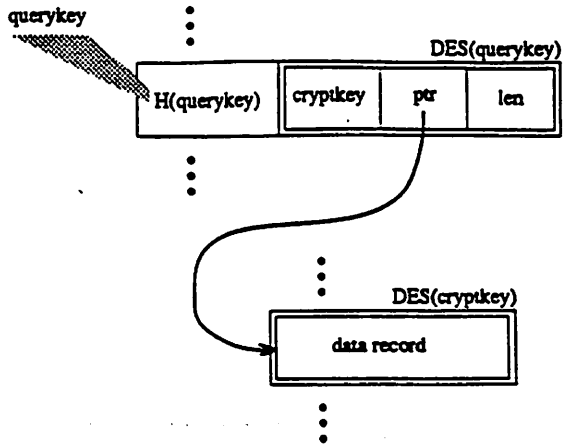


FIG. 1. *To allow searching by multiple keys, we use an indirect form of the usual encrypted database structure. Interpolation search using a hashed query key yields, after one deciphering step, a crypt key, pointer, and length. These are used, with a second deciphering step, to retrieve the data record.*

```
P'(k, L')
    {
        k' ← h(k)
        for all v' such that (k',v')∈ L'
            output(Dec(v',k))
    }
```

Since the hashed keys are uniformly distributed, the **for** loop only requires a (very fast) interpolation search.

In our application, the values $v_1, \ldots, v_n$ are the membership records. That is, v_i contains the name, address, phone number, etc. for the i^{th} member. The standard table-encryption technique assumes that the key-value relation is one-to-one. This is a problem because in our case, we wish to retrieve a record by the last name, which may correspond to multiple records. More importantly, we may wish to allow access to records by other keys as well.

Consequently we insert a layer of indirection. Let $v_1, \ldots, v_n$ be a list of membership records and $S_1, \ldots, S_n$ be the corresponding sets of keys. For example, we later choose S_i = {last name, phone number} of the member in record v_i. Let $r_1, \ldots, r_n$ be a list of random numbers. The encrypted membership list contains records $E_1 = Enc(v_1, r_1)$. $\ldots, E_n = Enc(v_n, r_n)$. These variable length records are stored in a block of memory that we will refer to as *MainTable*.

Let $K_{in} = \{k_1, \ldots, k_m\} = \bigcup_{i=1}^{n} S_i$. A second block of memory, referred to as *AuxTable*, contains the fixed length records $(h(k), w = Enc(\Lambda, k))$ sorted in increasing order by $h(k)$ values. Each Λ is a list of triples of the form (r, a, l): r is the random number associated with a membership record v that has key k; a is the address of v in *MainTable*; l is the length of record v. So if k is the last name Cohen, Λ is a list of the random numbers, addresses, and lengths of all records of members named Cohen. The

contents of *AuxTable* and *MainTable* are summarized in Figure 1.

The lookup program P' becomes

```
P'(k, AuxTable, MainTable)
    {
        k' ← h(k)
        if k' ∉ AuxTable, return(∅)
        j ← index of k' in AuxTable
        Λ ← Dec(w[j], k)
        for (r, a, l) ∈ Λ
        {
                v' ← MainTable[a, a+l-1]
                output(Dec(v',r))
        }
    }
```

There is a small cheat here. The hash function h is in general not one-to-one, and hence k may not be the correct decryption key for w_j. A practical implementation therefore checks that a points inside *MainTable* and that l is not too large; if it is paranoid, it also verifies that k really is a key for each decrypted record v.

An organization can distribute the lookup program P' along with the membership information stored in *AuxTable* and *MainTable*. Because the membership records are distributed in encrypted form, they cannot be used directly for illegitimate purposes such as the generation of sales lists. Of course, an attacker could produce a complete set of cleartext records by exhaustively searching the keyspace. This weakness is unavoidable if the lookup program is to meet its specifications. In this application, the level of security appears to be appropriate to the level of the threat.

3. Example: The SIAM Membership List. By special arrangement, SIAM periodically sends netlib a dump of its member database. Currently there are 8176 records, with an average size of 95 bytes (name, address, phone number, and email address) for a total of 777 kilobytes. The most common last name, Chan, matches 44 records. Note that one copy of the list fits on a floppy disk, but two copies (as would be needed by naive table encryption) do not fit.

A practical realization of P' requires the choice of the hashing and encryption functions *h*, *Enc*, *Dec*. Since we wish to abide by both the letter and the spirit of stringent United States export laws, this choice was in fact the biggest hurdle of the project. (Export is important because SIAM is an international organization and, besides, netlib has no way to verify the destination country of email.) Ultimately, we chose the Data Encryption Standard (DES) [D82, M89] for all three functions. Many Unix^{TM} systems are delivered with library functions for this, so our program uses the library and does not include DES code. Fortunately, a DES implementation by Stig Ostholm of Finland is publicly available by anonymous ftp from `chalmers.de` as file `ftp/pub/des`. The lookup program we distribute only uses DES in one direction, so there is no point trying to use it for encrypted communication.

In the United States, a ten digit telephone numbering scheme is used that currently allows about 10,000 valid six digit prefixes. To exhaustively try all phone numbers therefore takes roughly 10^8 tries. Let us postulate an attacker armed with a modern workstation and DES implementation that executes in ten microseconds. Decrypting one record is no help in cracking others, and our attacker's objective is the entire list. If the cost of the hash function were just one DES call, the 10^8 tries could be done in a few thousand seconds. That is unacceptable, so we use multiple rounds of DES. There is a delicate balance here between making lookup slow enough to discourage crackers with fast workstations, yet fast enough to allow quick response on a slow personal computer. At the present state of technology, about 30 rounds of DES per cipher operation is a reasonable tradeoff. (Twenty cpu days and a little programming skill would be needed on the hypothetical workstation.) Note that the multiple rounds of DES are only needed for hashing and for encrypting the pointer, not for encrypting the actual data. The distributed program reads the number of rounds from the database, to allow transparent change in later distributions of the database as computers get faster.

Another possible attack would be to try a list of common names. A list of 1095 most common last names from a Portland telephone book matched 1925 out of the total 8176 records in the SIAM example; a larger list of 18031 names from Bell Laboratories matched 3964 records. Even easier in this particular application would be to skip the encrypted database altogether and key or scan in the Combined Membership List published by the mathematical societies. Ultimately, we have to rely on the copyright notice attached to the database and the express prohibition against misuse. The purpose of the technical scheme is to dissuade casual attackers.

For details of implementation, the reader is invited to examine the code, which is available by

```
mail netlib@research.att.com
send decryptdb.c from 1127
send siamdb.uu from 1127.
```

This version of the database is a small sample from the start of the SIAM membership list. Since the encrypted file is binary, for email purposes it is shipped in a form that must be unpacked using the uudecode Unix system command. *(After the necessary approvals within AT&T and SIAM, the code and the full database will be moved to the public part of netlib, which also makes them accessible by anonymous ftp.)* Compile the C program; then to search for, say, Dr. Aavatsmark's entry

```
decryptdb siamdb Aavatsmark
```

The code is mostly a straightforward implementation of Figure 1. One subtlety is that decryption of the data record actually uses the "encrypt" direction of the `encrypt` library function. This is because some vendors provide a library that does not allow the "decrypt" direction.

The alternative to distributing membership lists is to provide remote access to a central database. The SIAM membership list has long been available in this way by sending a `whois` message by email to netlib. The AMS has recently begun to provide access to the mathematical societies' Combined Membership List by interactive ac...

over the Internet. These are popular services and should continue. One difficulty these alternatives do have is the startup delay. We dream of a day when your telephone, which already can tell you the calling number, will conspire with your local computer to tell you who belongs to that number, even if you've never had a call from him before.

REFERENCES

[D82] D. Denning. *Cryptography and Data Security*, Addison-Wesley, Reading, 1982.

[FLW89] J. Feigenbaum, M. Liberman, and R. Wright. Cryptographic Protection of Databases and Software, *Proceedings of the DIMACS Workshop on Distributed Computing and Cryptography* (Princeton, NJ; October, 1989), AMS/ACM, 1991, 161-172. Also available as AT&T Bell Laboratories 11276-900306-03TM.

[M89] R. Merkle. One-Way Hash Functions and DES, *Proceedings of the 9th CRYPTO* (1989), Springer-Verlag LNCS 435, 428–436.

[NY89] M. Naor and M. Yung. Universal One-Way Hash Functions and their Cryptographic Applications, *Proceedings of the 21st STOC* (1989), ACM, 33–43.

Notice Board

This space is new to the newsletter and is provided as a service to our membership. The editor's policy is to present information of interest to the membership of the IACR. Submissions are open to everyone. No paid advertising will be accepted and the editor reserves the right to reject any submissions.

Conference Calendar (bold face indicates IACR sponsored conferences)
EUROCRYPT'92 - May 24-28, 1992, Hotel Füred, Balatonfüred, Hungary, Conference Chair - Tibor Nemetz, Math. Inst. of the Hungarian, Acad. of Sci., P.O. Box 127/H-1364, Budapest, Hungary, email - h1137nem@ella.hu

CRYPTO'91 - Aug. 16-20, 1992, U.C. Santa Barbara, Conference Chair - Spyros Magliveras, Comp. Sci. Dept., Univ. of Nebraska - Lincoln, Lincoln, NE 68588-0115, USA., 402-472-5005, email - spyros@helios.unl.edu

AUSCRYPT'92 - Dec. 14-17, 1992, General Chair - William Caelli, Info. Security Research Centre, Queensland Univ. of Technology, GPO Box 2434, Brisbane, QLD 4001, Australia, +61-7-864-2752, fax +61-7-221-2384, email - w.caelli@aut.edu.au

Recent Thesis Submissions

The following are abstracts from recent thesis submissions.

Recently Accepted PhD Thesis
Lawrence Peter Brown, "Analysis of the DES and the Design of the LOKI Encryption Scheme", for Doctor of Philosophy, Department of Computer Science, University College, University of New South Wales, Australia, April 1991.
Supervised by Professor Jennifer R. Seberry, Dr. Ah Chung Tsoi, and Dr. David Anderson.
Abstract
This thesis will analyse some existing encryption algorithms used to provide secrecy in communications and data storage, and will detail the development of a new private key algorithm. It starts with a brief survey of modern encryption algorithms and their uses. It then takes a closer look at the RSA public key algorithm, with particular reference to its practical implementation. It shows that whilst RSA has some very desirable properties for use in public networks in that keys need not be exchanged previously, limitations in implementation speeds mean that RSA alone is not sufficient. Consequently a hybrid scheme is required which combines a public key scheme for authentication and key exchange, with a private key scheme for privacy. At present the DES algorithm is the sole certified private key scheme. It has been extensively analysed for possible weaknesses since its adoption in 1977. It is generally agreed that whilst the structure is sound, its key size of 56-bits has become too small with the improvements in computational speed on modern computers. Whilst the DES algorithm is public, its design criteria are classified. This thesis examines the design of the DES data encryption algorithm and related schemes, particularly with reference to the fundamental avalanche and completeness properties. From this is developed some possible design criteria for such schemes. Using these criteria, along with insights based on generic substitution-permutation cipher construction, suggestions and support from the authors colleagues, and with some results on substitution box design by Pieprzyk and Seberry, a new group of private key schemes, the LOKI family, is designed and presented as the major achievement of this thesis.

ON SCHLIEMANN, SHANNON & CERAM *(MAREK REVERSED)*

Schliemann provided the common sense, Shannon the theory and Ceram, along with a long list - Cleator, Cottrell, et Al - the fascination with the history of pre-UNI times. Horace C.2,2,11, tells us explicitly who the UNI was in the 1st century A.C.E.: Si uterque PoenI, serviat UNI. (Stress added)

While to understand the beautiful, elegant and astounding encoding system that I have broken over the years one need not know Latin; for the text itself one should have a background In some Italic variant - It., Sp., Fr., Port., or have a Latin informant. No smooth translation will be furnished; just a direct transcription from the Umbrian and a letter-aligned, stair-stepped, glossary with English definitions. The Smooth Translation field will be left in blank to be filled in by the individual or the team studying the document. This method will avoid endless haggling over one tiny bush in a huge forest of very important trees.

The first words/stems that literally popped off the page after I had carefully reversed the text, were: ARA-, XII, CARU-, DAMNE, NESCI, LARV-, AULE, CUNA, CENU-, ALMA, MA (Ma-gna Ma-ter), CACE (Eng. CACK, Ger.KAK-KANI AURA, ATENA, MI, ME. If the crytologian or his Latin informant is able to handle these and knows how his computer must be instructed to compute two high frequency heterographs, the single vertical strokes (2) & the continuous curves (2), a major hump is jumped. These four signs are separated because computer have not the human CONCEPT Of CONTEXT.

If the cryptologian is further able to apply the old PROLEPSIS to Shannon, i.e. bits used in advance of the byte that explains them, and is well aware of the the importance of Letter Frequency/Percentage In cryptanalysis, then one only has to learn a few new/old terms for pre-computer DATA COMPRESSION: Hapax, haplograph, stroke count, vinculum, umbilicus, Interpunctio(lacunae), apocopes, syncopes, acronyms, asterism, for a good start, the asterism being a compression of "pay special attention to what follows!," condensed to little more than a space, but saving 32 hand-carved letters as well as expensive polished-stone surface also.

A 2nd undecoded document awaits any bored, half-idling scientific mind, in retirement or out, that would appreciate the challenge and excitement of unlocking a 2,200 year-old voice. Contact Ben F. Blankenship, 510 820 - 7595, FAX 1 510 838-7536, or Box 2461, San Ramon CA 94583.

1992 Membership Application (Memberships Expire 12/92)
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 91 or Crypto 91 are already enrolled for the calendar year 1992. Payment on this form will bring Volume 5 of the Journal of Cryptology, whenever it is published.

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.0. Box 303
Palo Alto, CA 94302-0303
USA