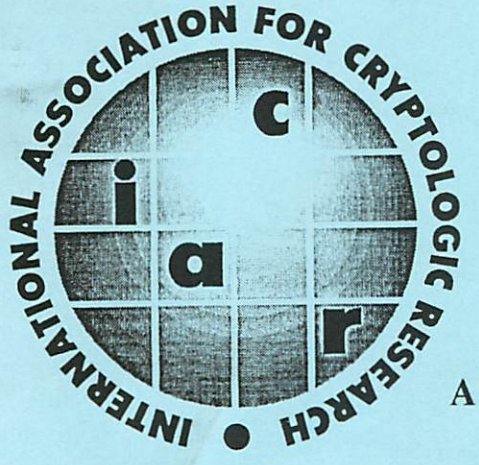

IACR

NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 10 Number 1 January 1993

CONTENTS

IACR Contact List

IACR Business Office
Aarhus Science Park
Gustav Wieds Vej 10
DK-8000 Aarhus C
Denmark

Officers . . .

President
Peter Landrock
IACR Aarhus Science Park
Gustav wieds Vej 10
DK-8000 Aarhus C
Denmark

Vice President
Ingemar Ingemarsson
Linkoping University
Dept. of Electrical Engineering
S-581 83 Linkoping
Sweden
+46 13 281 300
I2@isy.liu.se

Secretary
Sherry McMahan
1141 Venice Rd.
Knoxville, Tenn.
37923
+1 615 691 9218

Treasurer
Kevin McCurley
Div. 1423
Sandia National Laboratories
Albuquerque, NM 87185
USA
+1 505 845 7378
mccurley@sandia.gov

Eurocrypt 93 Chair
Kåre Presttun
Alcatel Telecom Norway AS
Box 255 Økern
N-0510 Oslo
Norway
47 2 63 82 47
email: kare.presttun@alcatel.no

Crypto 93 Chair
Paul VanOorshot
Bell Northern Research
P.O. box 3511, Station C
Ottawa, Ontario, Canada
K1Y 4H7
+1 613 763 4199
email: paulv@bnr.ca

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

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

Directors . . .

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

Bob Blakley
Mathematics Dept.
Texas A&M Univ.
College Station, Texas USA
77843-3368
+1 409 846 0523
email: blakely@math.tamu.edu

Andrew J. Clark
P.O. Box 1156
Brighton, East Sussex
BN1 5GT, United Kingdom
+44-273-566115 (tel/fax)

Yvo Desmedt[1]
Dept. of Elec. Eng. & Comp. Sci.
Univ. of Wisconsin - Milwaukee
P.O. Box 784, Milwaukee, WI
USA 53201

Whitfield Diffie
Sun Microsystems, MTV01-40
2550 Garcia Ave.,
Mountain View, CA 94043
USA
415 336 5414
email:whitfield.diffie@eng.sun.com

Hideki Imai
Elec. and Comp. Eng
Yokohama National University
156 Tokiwada, Hodogaya, Yokohama 240
Japan
+81 45 335 5036
imai@imailab.dnj.ynu.ac.jp

Jean-Jacques Quisquater
Avenue des Canards 3
B-1640 Rhode-Saint-Genese
Belgium

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[1]
Centre for Comp. Security Research
Dept. of Computer Science
University of Wollongong
Wollongong NSW 2500
Australia
jennie@cs.uow.edu.au

Scott Vanstone[1]
Dept. of C&O
Univ. of Waterloo,
Waterloo, Ontario, Canada
N2L 3G1
519 885 1211 X4063
email:savansto@math.waterloo.edu

[1] Shared term

Editor's Corner

Happy 1993. As most of you were aware, three directorhips were up for election this year. The official results are posted on the next page. I'd like to welcome the new and returning directors Whit Diffie, Bob Blakely and Jean-Jacques Quisquater (who will serve through 1995). Congratulations on the election results. I'd also like to give special thanks to the directors who have left the board - David Chaum and John Gordon. They have both served the IACR in many ways over the past years and it is their tireless efforts that have helped to bring the association to its present form. I'm sure that David and John will still be involved in the IACR for many years to come.

Also noted in the election results were our sincere appologies to Jennifer Seberry for an oversight on the election ballot. In the past, the IACR has maintained a very informal nature. The recent expansion of the IACR has caused us to formalize many of our administrative procedures. Our recent experience has pointed out the need to formalize the nomination procedures. This will certainly be done before the next election.

GBA

(**Please Note:** Due to events beyond my control, my email address has been changed to :

gbagnew@ccng.uwaterloo.ca

and mail to the old address is not being forwarded.)

ELECTION RESULTS

As returning officer for the IACR Election 1992 I declare the following:

The IACR Election Ballot 1992 was held to elect three directors of the IACR who will serve for a three year term from 1 January 1993 until 31 December 1995 inclusive. The closing date for receipt of completed ballots was 15 November 1992.

Six candidates stood for election and each polled the following number of votes;

Bob Blakley	117
David Chaum	65
Whitfield Diffie	149
Jean-Jacques Quisquater	107
Othmar Staffelbach	100
Stafford Tavares	61

Whitfield Diffie, Bob Blakley and Jean-Jacques Quisquater are duly elected as Directors of the IACR for the term 1 January 1993 until 31 December 1995 inclusive.

222 IACR members voted out of 624 eligible to vote. There were 15 spoiled (invalid) ballot papers submitted.

The nominations committee comprised Andrew J Clark (Returning Officer), Gordon Agnew and Yvo Desmedt. They would like to formally apologise to Jennifer Seberry who had planned to stand for election but, owing to an unfortunate misunderstanding, whose name was omitted from the ballot papers.

After the ballot papers had been distributed and the omission discovered, Jennifer decided that, in the best interests of the IACR, she would prefer to withdraw her name from the list of candidates rather than request that the election be re-run. The nominations committee acknowledge her support and understanding in this matter.

Andrew J Clark - 19 November 1992

Minutes of IACR BOARD of DIRECTORS MEETING
16 August, 1992

The meeting was called to order at 2:00 p.m. by the Peter Landrock, President of IACR. In attendance were Tom Berson (also with Andy Clark's proxy), Kevin McCurley, Gordon Agnew, Jennifer Seberry, Scott Vanstone, Ingemar Ingemarsson, Spyros Magliveras, David Chaum Yvo Desmedt, Ron Rivest, Hideki Imai, Whit Diffie and Sherry McMahan.

AGENDA: The agenda was reviewed and Jennifer Seberry made a motion to add to the agenda the reconsideration of the logo. The motion was seconded by Yvo Desmedt. The vote: for-7, no-0, abstain-1. The agenda was amended and the motion by Gordon Agnew was made to accept the agenda as amended, this was seconded. The vote: for-8, no-0, abstain-1.

EUROCRYPT '92: Written report has been received from Tibor Nemetz. Financial report along with complete set of books, accounting and money have been received by Kevin McCurley. There are still just a few loose ends but Tibor's quick reply is to be commended. Special thanks to Tibor for the great job.

CRYPTO '92: Spyros Magliveras reported that there are 218 registered as of today (25 not yet paid). Spyros mentioned the out of date mailing list, out of the 1800 announcements mailed 150 were returned. He also brought up the idea of a late fee. There was discussion among the members and Spyros made a motion to revise the General Chairman Guidelines to require a late fee for late registration and change wording for announcements for the Crypto conferences to reflect that late registrations will be accepted if space is available (however there are NO guarantees that space will be available.) Ingemar Ingemarsson seconded the motion. The vote: for-8, no-0, abstain-0.

Peter Landrock brought up the issue of the confusion caused by the wordings "sponsored by IACR..." and "in cooperation with IACR..." for the conferences such as Asiacrypt and Auscrypt. It was decided that there should be written instructions from the President of IACR to the conference chairman stating the exact wording to be used with each conference announcement, except for Crypto and Eurocrypt which are addressed in the Guidelines.

EUROCRYPT '93: The conference will be held in Norway from 24 to 27 May, 1993. Peter Landrock reported that all is on schedule and that the request for the mailing list has been received.

EUROCRYPT '94: Peter Landrock has written a letter to William Wolfowicz's boss announcing William as general chairman for Eurocrypt '94. Tentative dates are 22-25 May '94. It should be

noted that the IEEE/TC Security and Privacy conference is being held 15-20 May '94.

CRYPTO '93: Paul Van Oorschot has accepted as General Chairman. The dates are 22-26 August '93. Peter Landrock will speak with Paul about choice for program chairman. (Doug Stinson accepted as program chairman.)

CRYPTO '94: Peter Landrock to ask UCSB for the dates of 21-25 August '94 for Crypto '94.

NOMINATION COMMITTEE: Gordon Agnew reported that John Gordon does not wish to stand again for director of IACR. The following wish to stand: Othmar Staffelbach, David Chaum, Jennifer Seberry, Whit Diffie, Stafford Tavares and Jean-Jacques Quisquater. There is still time for others to be nominated and at the assembly Peter will ask for more nominations. Each candidate will be asked to submit two to three lines about himself to be included on the ballot.

ICSU AFFILIATION: After some discussion, there was a motion that IACR not continue to look at membership in ICSU. The motion was seconded and the vote: for-9, no-0, abstain-0.

LOGO: A revised logo was presented. Motion to accept and second received. Unanimous vote to accept revised logo.

It was decided that Kevin McCurley should write a letter to the artist and have all rights to the logo transferred to IACR.

Thanks to David Chaum and Tom Berson for all the work on the logo.

MAILING LIST: There was much discussion on the mailing list and the database to be used. Andy Clark has a database from Eurocrypt '91 and Peter Landrock will contact Andy about this. (After the meeting Andy Clark stated that he had a mailing list for Eurocrypt '91 which has now been destroyed in accordance with his agreement with the IACR President when the data was originally issued.)

It was recommended that the President should send a standard letter to each general chairman to accompany the soft copy of the mailing list stating that the use of this database is reserved for IACR use only and that the general chairman should acquire at the expense of the conference the appropriate required software to access the database. This should also be included in the General Chairman Guidelines.

IACR BOD minutes
16 August, 1992

BYLAWS: Sherry McMahan made a motion to set up a committee to review the Bylaws and Articles of Incorporation for possible amendment. Seconded by Tom Berson. Discussion on standing committee or not and why the need for review. The vote: for-8, no-2, abstain-1. Peter Landrock appointed the committee: Yvo Desmedt, David Chaum, Peter Landrock, Ingemar Ingemarsson, Whit Diffie, and Sherry McMahan (and possibly Jim Massey if he will join).

PROCEEDINGS: Kevin McCurley has not been able to do much in pursuing printing the proceedings elsewhere. Tom Berson wrote to Springer and received a letter stating the increase in proceedings over the next few years.

IACR has several options:

1) Keep things the way they are and accept additional costs (although the costs should be renegotiated with Springer);

2) Have only one proceeding - (no abstracts)

   a) Use Springer

   b) Negotiate with other publishers

There was much discussion for and against having both pre-proceedings (abstracts) and proceedings.

It was decided to look at other publishers and an Ad hoc committee was established by Peter Landrock. Members include Kevin McCurley (as chair), Tom Berson, Ron Rivest and Scott Vanstone. Tom to respond to Springer on 1992 rates and that the IACR will be looking at other possibilities.

Kevin McCurley made a motion to unbundle the price of proceedings from the conference fee. Seconded by Yvo Desmedt. Vote: yes-10, no-0, abstain 1. This will be done for Crypto '93.

A discussion followed on the scientific aspects of the proceedings, citeable references and whether the deadline for the papers for the proceedings should be required to be submitted within two weeks after the end of the conference. It was decided to have Yvo Desmedt and Ron Rivest look at the Program Chairman Guidelines to see if any of these ideas could be incorporated in the Guidelines. Yvo will have ready at Eurocrypt '93.

NATIONAL CHAPTERS OF IACR: It was decided to defer until a subsequent meeting the discussion of the desirability of national chapter of IACR.

IACR BOD Minutes
16 August, 1992

PANEL DISCUSSION AT CONFERENCES: This can be incorporated in the Program Chairman Guidelines.

NEW BUSINESS: It was decided at Eurocrypt '92 that the IACR membership fee will be $50 with no increase in student fees. Kevin McCurley is to report due changes to the General Assembly.

NEXT MEETING: Peter Landrock to look into having the Board of Directors, Eurocrypt '93 meeting in Bergen before boat cruise on 23 May.

Meeting adjourned.

Respectfully submitted,

Sherry S. McMahan
Secretary

IACR General Business Meeting
19 August, 1992

Peter Landrock called to order the general business meeting at 4:40 p.m. on 19 August. Peter reported that there are presently 620 IACR members. He introduced the directors and gave letters of appreciation to Spyros Magliveras (General Chairman-Crypto '92) and Ernie Brickell (Program Chairman-Crypto '92).

Mailing address for IACR is:

IACR Business Cf.
Aarhus Science Park
Gustav Wiells Vej 10
DK-8000 Aarhus C
Denmark
email: iacr@daimi.aau.dk

PRESENTATION OF LOGO: Peter Landrock presented the new IACR logo. A special thanks to David Chaum.

JOURNAL OF CRYPTOLOGY: Gilles Brassard presented report - Volume 4 in 1991 (work of Ernie Brickell). 1992 on schedule with Volume 1 and 2 mailed and 3 on time. Four issues for Volume 6. Springer has agreed to upgrade quality of reprints. When submitting articles for review via email once is enough but via mail need three copies.

Claude Crepeau is doing a special edition of the journal on Zero Knowledge.

CONFERENCES: Auscrypt '92, 13-16 December on Gold Coast, Queensland, Australia, Bill Caelli, General Chairman and Jennifer Seberry, Program Chairman.

Eurocrypt '93, 24 -27 May at Hotel Ullensvang, Lofthus, Norway. Kare Presttun, General Chairman and Tor Helleseth, Program Chairman. Registration by 1 April, 1993.

Crypto '93, 22 -26 August, UCSB, Paul Van Oorschot, General Chairman and Douglas Stinson, Program Chairman.

Eurocrypt '94, 22-25 May '94 (tentative date), Perugia, Italy, William Wolfowicz, General Chairman and Alfredo de Santis, Program Chairman.

NOMINATION FOR CANDIDATES FOR DIRECTORS OF IACR: There will be an election for three directors of IACR. Nominating Committee consists of Yvo Desmedt, Andy Clark (Chairman) and Gordon Agnew. Nominations close on 15 September with ballots mailed by 1 October and elections close by 15 November. Candidates to date: Whit Diffie, David Chaum, Bob Blakely, Jennifer Seberry, Othmar

IACR General Business Meeting
19 August, 1992

Staffelbach, Stafford Tavares and Jean-Jacques Quisquater. Nominations are open if anyone wishes to nominate anyone. Results of the election will be in the January '93 IACR newsletter.

FINANCIAL REPORT: Kevin McCurley spoke about the financial condition of the IACR and he presented the increase in dues. He spoke about the situation with the proceedings. Membership fee for 1994 (collected at conferences in 1993) will be $50.00. It was decided to vote on the requirement of two registration forms one stating the full price of the conference with the proceedings and one stating the price of the conference separate from the proceedings. Vote carried.

NEW BUSINESS: Open discussion with the following issues raised:

i) Bulletin Board for IACR (need further study)
ii) Proceedings mailed before conference (not possible due to time constraints).
iii) Rump Session - political, section with panel discussion, etc. (Covered in Program Chairman Guidelines).
iv) Request for an index of papers on cryptography. NIST published a table of contents-perhaps Miles Smid could follow to determine if this could be updated and distributed. Someone else requested a bibliography with Journal of Cryptology.
v) Circulation of Proceedings and Journal
vi) Peter Landrock mentioned that this is the 12th Crypto conference and he wished to give special recognition to several members of IACR. Special recognition of attendees at the first Crypto-these are: Tom Berson, Whit Diffie, and David Chaum and attendees at the first Eurocrypt: Whit Diffie and Andy Odlyzko. Special recognition for authors with at least ten papers accepted at Crypto-these are: Jean Jacques Quisquater, Yvo Desmedt and Ernie Brickell. Special recognition for those individuals which have attended the most Crypto and Eurocrypt conferences (including Auscrypt and Asiacrypt), these are: Jennifer Seberry (with the most), Sherry McMahan (second) and Kenji Koyama.

Meeting Adjourned.

Respectfully submitted,

Sherry S. McMahan
IACR Secretary

CONFERENCE ANNOUNCEMENT

EUROCRYPT '93
May 23-27, 1993
Hotel Ullensvang, Lofthus, NORWAY

A Workshop on the Theory and Applications of Cryptographic Techniques

Sponsored by the International Association for Cryptologic Research (IACR)

EUROCRYPT '93 continues the tradition of European IACR conferences dedicated to the theory and applications of cryptographic techniques. Please turn over to the Call for Papers for a detailed description of the scientific content.

EUROCRYPT '93 will be held between 23-27 May 1993 at Hotel Ullensvang in Lofthus, Norway. The scientific program will start Monday morning and close Wednesday afternoon. There will also be a rump session on Tuesday evening for informal presentations. The social program includes a reception at the Sima Hydropower Plant on Monday and a conference banquet on Wednesday evening.

The conference site, Lofthus, is located at the southern shore of Hardangerfjord, 10 km from Kinsarvik. The fjord is surrounded by snow-clad mountains and welcomes you to one of the most scenic parts of the country. There are excellent possibilities for interesting walks and trips in the near surroundings as well as for boating on the fjord. This district is famous for cultivation of apples and the blossom should be at its peak during the conference. The weather in this region is normally good at this time of the year and the temperature is expected to range from 15 to 20 degrees C in daytime.

The hotel itself provides excellent conference facilities as well as possibilities for indoor swimming, tennis, squash, badminton and bowling.

Transport: Lofthus is about 140 km from Bergen and 360 km from Oslo. It will be possible to join a common transport by boat from Bergen in the afternoon of Sunday May 23. A bus transport to Bergen will be organized after the conference. There are daily connections to Bergen Airport from Copenhagen and London, and more than 10 daily connections from Oslo airport. Lofthus can be reached from Bergen and Oslo using train and bus.

Predicted hotel prices:
Single/double/triple room 850/600/500 NOK per night incl. breakfast. The accommodation will be shared between Hotel Ullensvang and Fjordhotel Kinsarvik. Cheaper accommodation for students will be provided. (250/350 NOK)

Predicted registration fee: 2850 NOK (Students 2200 NOK).

IMPORTANT DATE: The deadline for registration will be **April 1, 1993.**

Additional information and a registration form will be sent to attendees of previous Eurocrypt and Crypto conferences around January 15, 1993. For further information, and to make sure you are on the mailing list, write to the conference address.

ORGANIZING COMMITTEE: Kåre Presttun (Alcatel Telecom Norway) (general chairman), Leif Nilsen (Alcatel Telecom Norway), Øystein Rødseth (University of Bergen),Torleiv Kløve (University of Bergen), Øyvind Ytrehus (University of Bergen), Kenneth Iversen (KITH)

FURTHER INFORMATION

Eurocrypt '93
Box 255 Økern
N-0510 Oslo
Norway

Phone: +47 2 638447
Faxsimile: +47 2 638497
E-mail: eurocrypt93@alcatel.no

REGISTRATION FORM EUROCRYPT '93

May 23 -27, 1993 - Hotel Ullensvang, Lofthus Norway

The deadline for registration is 1st April 1993

Last Name: _____ First Name: _____

Accompanying person: _____

Address: _____

_____ Sex: (M/F) _____

_____ Tel: _____

_____ Fax: _____

Country: _____ Email: _____

I shall be attending Eurocrypt '93 and wish to register for the conference and the following facilities:

Conference Fee:	Regular (NOK 2700)	NOK	_____
	Full-Time Student (NOK 2000)	NOK	_____
	Late registration fee (NOK 3500)	NOK	_____
Accommodation:	In single room (NOK 850/night/pers)	NOK	_____
	Double room (NOK 600/night/pers)	NOK	_____
	Triple room (NOK 500/night/pers)	NOK	_____
	Student lodging (NOK 250/night/pers) Limited number of double rooms available.	NOK	_____
Social events:	_____ tickets for Sima (NOK 260)	NOK	_____
	_____ additional Banquet tickets (NOK 600)	NOK	_____
Airport Travel:	Boat from Bergen to Lofthus Sunday (NOK 175)	NOK	_____
	Bus from Lofthus to Bergen Thursday (NOK 100)	NOK	_____
I cannot attend but require _____ copies of the pre-proceedings (NOK 350)		NOK	_____
TOTAL FEE ENCLOSED (This fee is NOT Returnable)		NOK	_____

I will accept accommodation in double room (Y/N) with preference of roommate : _____

YOUR PAYMENT MUST BE IN NORWEGIAN KRONER DRAWN ON NORWEGIAN BANK OR INTERNATIONAL MONEYORDER PAYABLE IN NORWEGIAN KRONER TO EUROCRYPT '93.

Send it to:
Eurocrypt '93
P.O.Box 255 Økern
N-0511 Oslo
Norway

Payment of the conference fee entitles you to become a member of the IACR. Do you wish to be an IACR member? ___ (Y) ___ (N)

Special dietary requirements? _____ (Y) _____ (N)
If Y, give information : _____

EUROCRYPT '93

Hotel Ullensvang, Lofthus, Norway
May 23-27, 1993

A Workshop on the Theory and Applications of Cryptographic Techniques

PRELIMINARY PROGRAMME

Sunday May 23rd

1500 - 2300	Registration at Hotel Ullensvang.
1530	Boat departure Bergen
1730	Boat departure Flesland
2100	Boat arrival Lofthus
2000 - 2300	Evening snacks.

Monday May 24th.

0900	Opening of the conference.
0915 - 1200	Lectures with coffee break
1215 -	Lunch in the hotel
1400 - 1800	Lectures with coffee break
1900	Departure for Sima hydro power plant.
2000 - 2200	Reception at Sima (NB! This is not included in the conference fee)

Tuesday May 25th.

0900	Opening of the conference.
0915 - 1200	Lectures with coffee break
1215 -	Lunch in the hotel
1400 - 1800	Lectures with coffee break
2000 -	Rump session. (Included in the conference fee)

Wednesday May 26th.

0900	Opening of the conference.
0915 - 1200	Lectures with coffee break
1215 -	Lunch in the hotel
1400 - 1800	Lectures with coffee break
2000 -	Banquet dinner at the hotel. (Included in the conference fee)

Thursday May 27th.

0900	Bus departure from the hotel.

SOCIAL PROGRAMME

Sunday May 23: The boat will arrive at about 21h00 at the hotel, registration and evening snacks is planned for the evening.

Monday May 24: In the evening there will be the excursion to Sima, the largest hydroelectric in Europe. After a guided tour around there will be a reception deep inside the mountain. Please observe that this tour is not included in the conference fee.

Tuesday May 25: This evening we have the traditional rump-session with food and drink served, and enjoyable presentations.

Wednesday May 26: This evening there will be a banquet in the hotel dining-room.

Programme for accompanying persons will be arranged by the hotel upon request.
Examples include:

- Visit to Agatunet, a collection of old houses, the oldest from around 1300;
- Seaplane sight-seeing over the glacier and mountains.
- Troll-train in Måbødalen (Måbø valley) on the old road (the new is mostly in tunnels).

Together with the hotel we will try our best to make the stay enjoyable.

ABOUT BERGEN

If you plan to extend your stay in Norway, a stay in Bergen is recommended. This beautiful city offers many possibilities. Fløybanen is a must. This is a beautiful cable train trip to one of the mountains surrounding Bergen. 1993 is also the 150 anniversary of the famous composer Edvard Grieg, and May 19-31 there is a special music festival to his memory. The famous Bergen International Festival takes place June 2-15. Please contact Bergen Tourist Board for more information. When you arrive in Bergen, Turistinformasjon at Bryggen will answer all your questions.

Bergen Tourist Board
P.O. Box 4055, Dreggen
N-5023 Bergen
Norway

Tel: +47 5 313860
Fax: +47 5 315682

CRYPTO '93

Call for Papers

The Thirteenth 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, the Computer Science Department of the University of California, Santa Barbara, and Bell-Northern Research Ltd. (a subsidiary of Northern Telecom) will be held on the campus of the University of California, Santa Barbara, on August 22-26, 1993. 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 26, 1993, to the Program Chair at the address given below. A limit of 10 pages of 12pt type (not counting the bibliography or the title page) is placed on all submissions. Submissions must arrive on time or be postmarked no later than April 21, 1993 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.

Authors will be informed of acceptance or rejection in a letter mailed on or before June 21, 1993. A compilation of all accepted abstracts will be available at the conference in the form of pre-proceedings. Authors of accepted abstracts will be allowed to submit revised versions for the pre-proceedings. A revised abstract should contain only minor changes and corrections to the originally submitted abstract. All revised abstracts must be received by the Program Chair by July 16, 1992. **The 10 page limit will be strictly enforced for the pre-proceedings.**

Complete conference proceedings are expected to be published in Springer-Verlag's Lecture Notes in Computer Science series at a later date, pending negotiation.

The Program Committee consists of D. Stinson (Chair, Nebraska), M. Bellare (IBM T. J. Watson), E. Biham (Technion, Israel), E. Brickell (Sandia National Laboratories), J. Feigenbaum (AT&T), R. Impagliazzo (UCSD), A. Odlyzko (AT&T), T. Okamoto (NTT, Japan), B. Pfitzmann (Hildesheim, Germany), R. Rueppel (R^3, Switzerland), S. Vanstone (Waterloo, Canada).

Send submissions to the Program Chair:

Douglas R. Stinson, Crypto '93
Computer Science and Engineering Department
115 Ferguson Hall, University of Nebraska
Lincoln, NE 68588-0115 USA
Telephone: (402)-472-7791
Fax: (402)-472-7767
Internet: `stinson@bibd.unl.edu`

For other information, contact the General Chair:

Paul C. Van Oorschot, Crypto '93 (STOP 000)
Bell-Northern Research
P.O. Box 3511, Station C
Ottawa, Ontario K1Y 4H7 Canada
Telephone: (613)-763-4199
Fax: (613)-763-2626
Internet: `crypto93@bnr.ca`

1993 IEEE SYMPOSIUM ON RESEARCH IN SECURITY AND PRIVACY

May 24-26, 1993
Claremont Resort,
Oakland, California

Sponsored by the
IEEE Technical Committee on Security and Privacy
In cooperation with the
International Association of Cryptologic Research

Symposium Committee:

Teresa Lunt, General Chair
Cristi Garvey, Vice Chair
Richard A. Kemmerer, Program Co-Chair
John Rushby, Program Co-Chair

PRELIMINARY PROGRAM

MONDAY

9:00--9:30:	Welcoming Remarks: Teresa Lunt and Dick Kemmerer
9:30--10:30:	VIRUSES AND INTRUSION DETECTION Doug McIlroy, Session Chair
9:30--10:00:	Measuring and Modeling Computer Virus Prevalence Jeffrey Kephart and Steve White
10:00--10:30:	USTAT: A Real-Time Intrusion Detection System for UNIX Koral Ilgun
10:30--11:00:	BREAK
11:00--12:00:	CAUSALITY AND INTEGRITY George Dinolt, Session Chair
11:00--11:30:	Preventing Denial and Forgery of Causal Relationships in Distributed Systems Michael Reiter and Li Gong
11:30--12:00:	Message Integrity Design Stuart Stubblebine and Virgil Gligor
12:00--2:00:	LUNCH
2:00--3:30:	PANEL: Privacy Enhanced Mail Panelists: TO BE ANNOUNCED
3:30--4:00:	BREAK
4:00--5:00:	AUTHENTICATION PROTOCOLS: Teresa Lunt, Session Chair
4:00--4:30	Authentication Method with Impersonal Token Cards Refik Molva and Gene Tsudik
4:30--5:00:	Interconnecting Domains with Heterogeneous Key Distribution and Authentication Protocols Frank Piessens, Bart DeDecker and Phil Janson
6:00:	POSTER SESSIONS

TUESDAY

9:00--10:30:	TIMING CHANNELS: John Rushby, Session Chair
9:00-- 9:30:	Modelling a Fuzzy Time System Jonathan Trostle
9:30--10:00:	On Introducing Noise into the Bus-Contention Channel James Gray
10:00--10:15:	Discussant: TO BE ANNOUNCED
10:15--10:30:	Open Discussion
10:30--11:00:	BREAK
11:00--12:00:	INFORMATION FLOW: John McLean, Session Chair

11:00--11:30	A Logical Analysis of Authorized and Prohibited Information Flows Frederic Cuppens
11:30--12:00	The Cascade Vulnerability Problem J. Horton, R. Harland, E. Ashby, R. Cooper,W. Hyslop, B. Nickerson, W. Stewart, and K. Ward
12:00--2:00:	LUNCH
2:00--3:30:	PANEL: The Federal Criteria Panelists: TO BE ANNOUNCED
3:30--4:00:	BREAK
4:00--5:00:	DATABASE SECURITY Marv Schaefer, Session Chair
4:00--4:30:	A Model of Atomicity for Multilevel Transactions Barbara Blaustein, Sushil Jajodia, Catherine McCollum and LouAnna Notargiacomo
4:30--5:00:	Achieving Stricter Correctness Requirements in Multilevel Secure Database Vijayalakshmi Atluri, Elisa Bertino and Sushil Jajodia
5:00:	TC MEETING

6:00:POSTER SESSIONS

WEDNESDAY

9:00--10:30:	ANALYSIS OF CRYPTOGRAPHIC PROTOCOLS: Yacov Yacobi, Session Chair
9:00-- 9:30:	Trust Relationships in Secure Systems -- A Distributed Authentication Perspective Raphael Yahalom, Birgit Klein and Thomas Beth
9:30--10:00:	A Logical Language for Specifying Cryptographic Protocol Requirements Paul Syverson and Catherine Meadows
10:00--10:30:	A Semantic Model for Authentication Protocols Thomas Woo and Simon Lam
10:30--11:00:	BREAK
11:00--12:00:	SYSTEMS: Virgil Gligor, Session Chair
11:00--11:30:	Detection and Elimination of Inference Channels in Multilevel Relational Database Systems X. Qian, M. Stickel, P. Karp, T. Lunt and T. Garvey
11:30---12:00	Assuring Distributed Trusted Mach Todd Fine
12:00:	SYMPOSIUM ADJOURN

- ----------

Symposium Registration: Dates strictly enforced by postmark.

Advance Member (to 4/12/93) $240*

Late Member (4/13/93-4/30/93) $290*

*Registration must include IEEE number to qualify.

Advance Non-Member $300
Late Non-Member $370

Advance Student $50
Late Student $50

Mail registration to:

Cristi Garvey
R2/2104
TRW Defense Systems Group
One Space Park
Redondo Beach, CA 90278
(310) 812-0566

NO REGISTRATIONS BY EMAIL

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.

Recently Completed Theses

Title: On the Design and Security of Block Ciphers

Author: Xuejia Lai

Supervisor: Prof. James L. Massey

Institution: Swiss Federal Institute of Technology, Zürich

Abstract:

Secret-key block ciphers are the subject of this work. The design and security of block ciphers, together with their application in hashing techniques, are considered. In particular, iterated block ciphers that are based on iterating a round function several times are considered. Four basic constructions of an iterated cipher are studied.

The block cipher IDEA is proposed. This cipher is based on the new design concept of mixing different group operations on 16-bit subblocks. Using operations on subblocks facilitates the software implementation of the cipher. The regular structure of the cipher facilitates hardware implementation. The interaction of the three chosen "incompatible" group operations provides the necessary "confusion",and the chosen cipher structure causes the required "diffusion".

The security of iterated ciphers against Biham and Shamir's differential cryptanalysis is discussed. Differential cryptanalysis is described in terms of an i-round "differential". It is shown that the maximum probability of such a differential can be used to determine a lower bound on the complexity of a differential cryptanalysis attack. The concept of "Markov ciphers" is introduced. It is shown that the security of a Markov cipher against differential cryptanalysis is determined by the transition probability matrix created by the round function. A design principle for Markov ciphers is formulated, viz., that its transition matrix should be non-symmetric. Differential cryptanalysis of the IDEA cipher is performed partly by theoretical analysis of the relationship between the three chosen group operations and the properties of the MA-structure within the cipher, and partly by numerical experiments on "mini versions" of the cipher. The results suggest that the IDEA cipher is secure against differential cryptanalysis attack after only four of its eight rounds.

The application of block ciphers in constructing hash functions is also considered. Five different attacks on hash functions obtained by iterating a hash round function are formulated and examined. Relations between the security of such an iterated hash function and the strength of its round function are derived. Schemes for constructing hash round functions by using block ciphers are discussed and new hashing schemes using the IDEA cipher are proposed. Four attacks on three known hash schemes are presented by applying a new principle for evaluating the security of a hash round function.

Computer and Communications Security Abstracts
Pre-launch Announcement

Keeping up with research in the fields of computer and communications security is becoming a major chore. A conscientious researcher last year would have had to read well over 600 papers; and as the field grows, the problem can only get worse.

We are currently developing, with Cambridge University Press, an abstracting service designed to solve this problem.

Computer and Communications Security Abstracts will summarise research in computer security topics such as access control, database security, formal methods, distributed systems, biometrics, security management, risk management, contingency planning, legal issues, audit, and applications: and in communications security topics including stream and block cipher techniques, public key cryptography and computational number theory, complexity and theoretical cryptography, cryptanalysis, authentication, protocols, and applications.

Our mission is to provide abstracts of as much published research and development work as possible. This includes not just conference and journal papers, but also research reports and theses, and we will make a particular effort to report work which is published in languages other than English, or which for other reasons might escape the notice of the research community.

We expect that the first issue will be published in March 1993. There should be a dummy issue out at the end of this year, which will be sent, together with subscription information, to all people who attended Eurocrypt 92 or Crypto 92.

If you would be able to help us with the abstracting work, then we are very keen to hear from you. We are particularly short of reviewers who can produce English abstracts of Chinese and Japanese originals.

Although we will cover the main periodicals, such as the IEE and IEEE journals, the Journal of Cryptology, Cryptologia, Computers and Security, the Journal of Computer Security, and the major conference proceedings, we would suggest that authors of work published elsewhere - such as in the form of research reports - should send us an offprint to ensure coverage.

Ross Anderson (rja14@cl.cam.ac.uk)
University Computer Laboratory
Pembroke Street
Cambridge CB2 3QG, UK.