IACR

NEWSLETTER

A Publication of the International Association
for Cryptologic Research

Volume 10 Number 2 June 1993

CONTENTS

IACR Contact List

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

Officers . . .

President
Peter Landrock[1]
IACR Aarhus Science Park
Gustav wieds Vej 10
DK-8000 Aarhus C
Denmark
landrock@daimi.aau.dk
+45 86 20 2000
+45 86 20 2975 fax

Vice President
Ingemar Ingemarsson[1]
Linkoping University
Dept. of Electrical Engineering
S-581 83 Linkoping
Sweden
I2@isy.liu.se
+46 13 281 300
+46 13 139 282 fax

Secretary
Sherry McMahan[1]
1141 Venice Rd.
Knoxville, Tenn.
USA 37923
sherry@cylink.com
+1 615 691 9218 or 1 408 735 6674
+1 615 691 9217 fax

Treasurer
Kevin McCurley[1]
Div. 1423
Sandia National Laboratories
Albuquerque, NM 87185
USA
mccurley@cs.sandia.gov
+1 505 845 7378
+1-505-845-7442 Fax

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

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

Newsletter Editor
Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
gbagnew@ccng.uwaterloo.ca
+1 519 885 1211 x3041
+1 519 746 5515 fax

J. Of Cryptology Editor
Gilles Brassard
Dept. IRO
Universite de Montreal
C.P. 6128, Succ. "A"
Montreal, Quebec, Canada
H3C 3J7
brassard@iro.umontreal.ca
+1 514 343 6807
+1 514 343 5834 fax

Directors . . .

Thomas A. Berson[2]
Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94301
USA
berson@crvax.sri.com
+1 415 324 0100
+1 415 324 0120 fax

Bob Blakley[3]
Mathematics Dept.
Texas A&M Univ.
College Station, Texas USA
77843-3368
email: blakley@math.tamu.edu
+1 409 845 7939
+1 409 845 6028 fax

Andrew J. Clark[2]
Logica
Cobham Park
Downside Road
Cobham, Surrey
KT11 3LX
UK
+44 71 637 9111
+44 932 866 184 fax

Yvo Desmedt[1]
Dept. of Elec. Eng. & Comp. Sci.
Univ. of Wisconsin - Milwaukee
P.O. Box 784, Milwaukee, WI
USA 53201
desmedt@cs.uwm.edu
+1 414 229 6762
+1 414 229 6958 fax

Whitfield Diffie[3]
Sun Microsystems, MTV14-203
2550 Garcia Ave.,
Mountain View, CA 94043
USA
email:whitfield.diffie@eng.sun.com
+1 415 336 5414
+1 415 336 4802

Hideki Imai[2]
Elec. and Comp. Eng
Yokohama National University
156 Tokiwada, Hodogaya, Yokohama 240
Japan
imai@imailab.dnj.ynu.ac.jp
+81 45 335 5036

Jean-Jacques Quisquater[3]
UCL
Dept. of Elec. Eng.
Place du Levant, 3
B-1348 Louvain-la-Neuve
Belgium
quisquater@dice.ucl.ac.be
+32 10 47 2541
+32 10 47 8667 fax

Ronald Rivest[1]
MIT Lab for Computer Science
545 Technology Square
Cambridge, MA 02139
USA
rivest@mit.edu
+1 617 253 5880
+1 617 258 8682 fax

Jennifer Seberry[1]
Centre for Comp. Security Research
Dept. of Computer Science
University of Wollongong
Wollongong NSW 2500
Australia
jennie@cs.uow.edu.au
+61 42 21 4327 or +61 42 26 9726
+61 42 21 4329 fax

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] Term expires Dec. 1993

[2] Term expires Dec. 1994

[3] Term expires Dec. 1995

Editor's Corner

Looking out my office window, I see that summer has finally arrived in Canada. That means it must be June and time for another newsletter editorial. Many things have happened over the past six months - some may have significant impact on the future directions of cryptologic research.

On the bright side, there was Eurocrypt '93. The conference was a great success. The venue was amazing; the fjords, the sunshine and the fabulous food. In all, there were 272 attendees. For those who did attend, I'm sure you'll join with me in thanking Kåre, Leif, Tor, and all of the others who worked so hard to make the conference a success. As for the rest, there's always next year in Perugia, Italy.

This year is an election year for both directors and the officers of the IACR. In the past, nominations and elections have been carried out in a rather informal way. Perhaps it's our coming-of-age that requires new guidelines to formalize the nomination and elections procedures. Later in this issue, the new procedures are explained along with new nomination forms.

There has been a lot of controversy over the introduction of a new secret key cryptosystem by the U.S. government. This system (Clipper) is intended for use in secure voice/data communications. It also employees a key escrow system to allow law enforcement agencies to tap selected communications (presumably with a court order). The extremely short time given by the government for public discussion and evaluation of this system is a source of great concern for the IACR and the cryptographic community. This has led the Board of Directors of the IACR to put forward a public statement expressing our concern (see the Minutes of the Board of Directors meeting, later in this issue).

GBA.

President's Message

Dear Members,

I wonder how many scientific societies experience such an activity and interest from the majority of its members as IACR. Enough to put together three conferences in one year: Two sponsored by and one (this time Auscrypt) in association with IACR.

Did you ever consider how much effort and good will this takes from the volunteers behind all these conferences? Every time, many members put hundreds of hours into the arrangement of just one conference. Most attendants seem to appreciate it very much. A few are more concerned with the tourist attractions, and will certainly point out if they had expected to see something else at the excursion. But, the vast majority of our participating members seems like fish in water at these conferences. Some do not even notice what they are eating, busy as they are with professional discussions, solving new problems, asking new questions, etc. Others do not notice what they are drinking. They get drunk and solve their problem, but have forgotten the next morning!

Anyway, there is more to it than that. Our Journal is thriving, thanks to a great lot to our extremely able chief editor, Gilles Brassard. A great "Cheers" to him. As you read these lines, Tom and I are busy trying to see if we can persuade Gilles to stay yet another period. You may have forgotten, but this year we have moved to four issues in each volume. Nevertheless, there are no shortage of papers, and things are running on schedule!

A few words on the conference within the last year:

CRYPTO'92 was organized by Spyros Magliveras, who had come up with a really unusual and relevant T-shirt as the gift for everybody. Ernie Brickell was program chair, and we had about 218 participants. The beach party was brought back into the program, and the scientific quality was characterized by broadness and hard work. A warm thank to the organizers. Just another great CRYPTO!

Then came the 2nd Auscrypt, with Bill Caelli as General Chair, and Jennifer Seberry as the Program Chair, at the nice quiet Somerset College on the Gold Coast south of Brisbane, with over 100 in attendance, (dominated by Europeans). I was there myself for the first time, but not the last! Thanks to the organizers, everything ran very smoothly, and we all learned how to dance the Polynesian style (at least, I tried).

Finally Eurocrypt'93 at Lofthus, Norway (next to paradise), with a stunning 272 participants. The hotel was a delight, and the organizers Kaare Presttun and Leif Nilsen had done the utmost to made sure everything worked. The program chair, Tor Helleseth had wisely conducted everything from Santa Monica. Of course, he spent a great deal of his sabbatical with this, but who cares? Several people told me this was the best conference ever, others that things were too expensive, and that there should be a warning on beer without alcohol. KGB and CIA were there (according to a local newspaper). Who wasn't?

Well, Gord is pulling my bitstring. See you in less than two months in Santa Barbara! I hope you prove a great theorem in the meanwhile.

Peter Landrock

Election of Officers and Directors of IACR
Nominations Procedures

IACR Nominations Committee (see inside front cover for addresses)
Tom Berson
Andy Clark (Returning Officer)
Gord Agnew (Chair)

Positions for this Election

Post	Term	Incumbent
President	Jan. 1994 - Dec. 1995	Peter Landrock
Vice President	Jan. 1994 - Dec. 1995	Ingemar Ingemarsson
Secretary	Jan. 1994 - Dec. 1995	Sherry McMahan
Treasurer	Jan. 1994 - Dec. 1995	Kevin McCurley
3 Directors	Jan. 1994 - Dec. 1996	

Nominators and Nominees must be **regular** members of the IACR. A member may be nominated for a position as an officer of the IACR and also as a director. In the event that the candidate is elected as an officer, their name will be removed from consideration (in the counting of ballots) as a director. Candidates may submit a statement of **up to 50 words in length** which will be included on the election ballot form.

DATES:

Nominations must be **faxed or mailed** to be received no later than **SEPT. 15, 1993**. Candidates' Statements must be faxed or mailed to be received no later than **SEPT. 20, 1993** (note: no email or hand delivered "forms" will be accepted at CRYPTO'93).
All correspondence must be directed to:

Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
gbagnew@ccng.uwaterloo.ca
+1 519 885 1211 x3041
+1 519 746 5515 fax

Nominations and Statements will be acknowledged by fax within two (2) working days of receipt (before the deadlines). It is the responsibility of the candidates to ensure that nominations and statements are received!

Ballots will be mailed by **OCT. 1, 1993**. Ballots must be mailed to be received by the Returning Officer in the official envelopes by **NOV. 15, 1993.**

IACR ELECTION NOMINATION FORM

I nominate ______________________________ for the position(s) of

______________________________.

Nominator:

______________________________ ______________________________

NAME (PRINT) SIGNATURE

______________________________ ______________________________

DATE FAX NUMBER

______________________________ ADDRESS: ______________________________

EMAIL ADDRESS ______________________________

I ______________________________ accept the nomination for the above position(s).

CANDIDATE'S STATEMENT: ______________________________

____

____

Nominee:

______________________________ ______________________________

NAME (PRINT) SIGNATURE

______________________________ ______________________________

DATE FAX NUMBER

______________________________ ADDRESS: ______________________________

EMAIL ADDRESS ______________________________

RETURN THIS FORM BY MAIL OR FAX TO:

Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
gbagnew@ccng.uwaterloo.ca
+1 519 885 1211 x3041
+1 519 746 5515 fax or +1 519 746 3077 fax

IACR BOARD OF DIRECTORS MEETING EUROCRYPT '93

The 1993 Eurocrypt IACR Board of Directors meeting was called to order by the President, Peter Landrock, at 11:00 a.m. at SAS Royal Hotel in Bergen, Norway on 22 May, 1993. In attendance were Bob Blakley, Gordon Agnew, Tom Berson, Yvo Desmedt, Ron Rivest, Jean Jacques Quisquater, Peter Landrock and Sherry McMahan. Proxies for Kevin McCurley and Gilles Brassard were given to Tom Berson, proxy for Andy Clark was given to Sherry McMahan (Andy will be arriving later), and proxy for Scott Vanstone was given to Gordon Agnew. Ingemar Ingemarsson, Whitfield Diffie, Paul Van Oorschot and Andy Clark will be arriving later. Jennifer Seberry had been asked to attend to speak on behalf of Hideki Imai who was unable to attend the meeting. (*Secretary's note concerning proxies - all proxies will be recorded as abstentions unless specifically voted.*)

Gordon Agnew moved to accept the agenda with one modification, add adjournment. This was done and the agenda was accepted as modified.

WELCOME BY THE PRESIDENT: Peter Landrock welcomed the new directors to the meeting Jean Jacques Quisquater and Bob Blakley (elected in the last election). Whitfield Diffie returned as a director.

1992 ELECTIONS: Gordon Agnew gave the report on the last election, which was as reported in the January 1993 IACR newsletter. Gordon also reported that there were several concerns about the election: 1) Jennifer Seberry's name was omitted from the ballot; 2) David Chaum did not submit a few lines about himself for the ballot; and 3) Bob Blakley's name was misspelled on the ballot. The nomination and election committee expressed apologies to each of these individuals. Gordon has some suggestions for procedures that would help avoid these mistakes in the future. These will be presented to the board later in the meeting.

CRYPTO'92: Spyros Magliveras was not present to give the report. There were 221 in attendance.

AUSCRYPT'92: Jennifer Seberry (Program Chair for Auscrypt '92) reported that there were over 100 in attendance with 16 countries represented. There were 77 papers submitted from 19 countries. Most was from Europe with second largest amount from Asia. Jennifer expressed thanks to the program committee. Peter mentioned that at Auscrypt there was a problem with the IACR membership fee. The fee had been set several months before the conference for the amount of Australian $50. However with the fluctuation of the exchange rate, the amount sent to IACR was Australian $50 per person which instead of US$40.00 was US$33.75 per person.

There was a discussion about what to do to avoid this situation with future conferences. Several suggestions were discussed. It was decided that the president would include a word of caution to the General Chair for Eurocrypt and other conferences where IACR membership is involved stating that the IACR membership dues are $50.00 U.S. and the Chair should consider ways to ensure that this amount is what is collected and sent to the IACR.

FINANCIAL STATUS: Tom Berson gave the report on behalf of Kevin McCurley. Tax filing was delayed for the year of 1992 until 20 June due to the late filing of information from CRYPTO '92 and Eurocrypt '92. The IACR is stable but the funds are not growing. It appears that there are several issues to discuss with Kevin about the financial report

1) clarification on what is needed to wrap up EC '92 and

2) details of income and expenses for non conference activities. Peter will contact Kevin over the next few days and ask Kevin about these issues and tell him that a complete financial report will be needed for the June IACR newsletter.

The board discussed the authorization for Kevin to invest the IACR monies at better interest rates. It was decided that Kevin should be authorized and encouraged to invest one half of the money for one half year at a better interest rate. Peter will notify Kevin of this.

When the Board meets again at 12:00 noon on Wednesday, Peter will give an update on the financial report.

JOURNAL OF CRYPTOLOGY: Report was given by Tom Berson on behalf of Gilles Brassard. "In a nutshell all is going well. Publication has kept on schedule despite the increase to four issues per year. Volume 6, number 1 has appeared and has nominally been received by our readers; Volume 6, number 2 is about to be printed. Moreover, there are enough papers already typeset to wrap up all of 1993. More precisely, there are 8 papers (138 pages) that are already typeset (not counting those already scheduled for Volume 6, number 2). In addition, 4 papers are ready to send to Springer for typesetting and 2 more are accepted but are waiting for final minor revisions from the authors. Finally, the paper flow has been consistently increasing: 25 papers were submitted in 1991 (which was low compared to the best pre1991 years), 34 in 1992, and 12 in the first 4 months of 1993".

"Here is a more detailed analysis of the current situation. Thirteen (13) papers are still left over from those submitted in 1990 or earlier, meaning that they have not yet been rejected nor have they appeared. Of those, 4 are inactive (not heard from the authors in at least one year), 3 will appear in the next issue (Volume 6, number 2), 2 are typeset and likely to appear in the following issue, 1 is ready to send to Springer for typesetting and 'only' 3 are still in refereeing limbo or waiting for revisions from their authors." Gilles said that he had several important items to deal with this year including the electronic treatment of the papers up to and including typesetting. Another is whether and when to go to four 64 page issues per volume instead of two 64 pagers and two 48 pagers".

Thanks to Gilles for his report.

The board will need to address at CRYPTO '93 the appointment of the Editor in Chief for the Journal. Peter will speak with Gilles about this. An Ad Hoc committee was formed with Peter and Tom to speak with Gilles and if necessary to consider other nominations.

Gilles will need to be prepared to present to the board at CRYPTO '93 a recommendation on if and when to go to four 64 page issues per volume. Kevin will also need to be prepared to look at the financial implications.

STRICTER PROCEDURES: Peter expressed concerns about stricter procedures needed for nominations and elections, membership, etc.. There was discussion about creating guidelines stating the procedures, similar to the General Chair and Program Chair Guidelines that already exist. After much discussion it was decided that the Bylaws need to be reviewed (Peter, Sherry and Ingemar to review Bylaws); Yvo will review Program Chair Guidelines for possible revision; 3) Nomination/Election Guidelines will need to be established Gordon Agnew to be responsible; and 4) General Chair Guidelines Jennifer to review for possible revision. Peter will arrange for electronic copies of the Bylaws and other guidelines to be sent to the respective individuals. Each individual will need to prepare the documentation for review by the board by 22 July. These should be sent by email to all board members. The board should come to CRYPTO '93 prepared to discuss and make decisions concerning each of these guidelines and Bylaws.

AD HOC COMMITTEE ON PROCEEDINGS: Tom reported that there has been no progress. (Kevin is chair, Tom, Ron and Scott are on this committee.) Tom spoke with Springer about 1992 rates. Peter has discussed with Springer about publications. The Committee is to come to CRYPTO '93 with a proposal on how the proceedings and preproceedings will be handled at subsequent conferences.

NOMINATION COMMITTEE: Gordon will serve as Chair for the nomination committee for the '93 elections. Andy and Tom will also serve on the committee. Gordon will prepare a nomination form for the June '93 newsletter. All nominations will need to be made in writing and confirmed in writing by the individual nominated. All officers and three directors positions will be open for this election. The directors serving in those positions now are Yvo Desmedt, Scott Vanstone and Ron Rivest. Gordon stated that all officers and the three directors names will automatically appear on the ballot unless the individual specifies otherwise.

NEWSLETTER: Report from Gordon Agnew is that all is going well.

There was a motion by Tom to appoint Gordon Agnew as Newsletter editor for one year. Bob seconded. Vote: For 8; no 0; abstain 1 (5).

EUROCRYPT '94: William Wolfowicz has brought over 250 announcements to be given out during EC '93. There has been discussions with Peter and Kevin concerning the bank account for the conference, however all issues have been resolved. The conference will be from 10 - 12 May, 1994 in Perugia, Italy. The welcome reception will be on Monday, 9 May, with the rump session on Tuesday night and the banquet on Wednesday. The session will go all day on Thursday and buses will be available to return to Rome on Thursday evening. William has been able to obtain several donations and stipends to support the conference. The deadline for registration is 1 April, 1994 with the hotel reservations to be made by 31 March. There was a discussion about the IACR membership fee and how it will be determined in order to protect the association from a depreciation of the lira to the dollar. Peter will give William the mailing list.

EUROCRYPT '96 PROPOSAL: Jose Pastor presented the city of Zaragoza, Spain as the proposed venue for EC '96. The conference would be sponsored with the Asociacion Espanola de Criptologia and Departamiento de Ingenieria Electrica & Informatica, Centro Politecnico Superior. Jose needs a budget format to complete and submit to the board for consideration at EC '94. Jose would be general chair. Program chair has not been determined.

EUROCRYPT '93 UPDATE: Kare Presttun reported that 267 have registered for EC '93. The conference is on budget. There were 117 papers submitted with 35 accepted.

There was a discussion on what to do about the proceedings. Andy Clark made the following motion:

> *The cost to print and distribute the proceedings for Eurocrypt '93 by Springer will be covered by the excess funds from Eurocrypt '93. Any additional funds required will be obtained from the IACR's general funds. The proceedings will be available at no additional charge only to participants of EC '93. The motion was seconded by Tom Berson. Vote: For 10; against 1; abstain 0 (3). Tom will make an announcement at the General Assembly. Peter and Tor to contact Springer.*

MEMBERSHIP RENEWALS: This will be addressed by the individuals reviewing the Bylaws.

IACR LETTERHEAD AND SEAL: Discussion followed about the seal and it was decided that Tom will check on obtaining a corporate seal for IACR. Peter will provide the logo in postscript form for all those who need it.

CRYPTO '93: Paul Van Oorschot reported that all is on schedule. Increase in conference fee is for increased membership fee and cost of proceedings. Paul had several concerns about stipends, etc. that will be passed on to Jennifer to include in the General Chair guidelines. Date of CRYPTO '93 is 22 to 26 August, 1993 at UCSB.

CRYPTO '94 GENERAL CHAIR: Each board member is to bring one name to nominate for GC for C '94 to the BOD meeting on Wednesday, 26 May at 12:00 noon.

ASIACRYPT '94: Jennifer Seberry presented a request for IACR's participation in Asiacrypt '94 as "*in cooperation with*". The conference will be held in Woologong, NSW, Australia in December '94. Program chair will be Josef Pieprzyk. A motion for Asiacrypt '94 to be "in cooperation with IACR" was made by Gordon Agnew. Second by Ingemar Ingemarsson. Vote: For 11, No 0, abstain 0 (3).

"*IN COOPERATION WITH*" STATUS: Peter Landrock said that he had been contacted by Ravi Ganesan of Bell Atlantic for the 1st ACM Conference on Computer and Communications Security from 3 - 5 November, 1993 in Fairfax, Virginia to be in cooperation with IACR. Peter determined that was okay. Peter asked the board to ratify his decision. Tom Berson made a motion to ratify the decision. It was seconded by Yvo Desmedt. Vote: For 11, No 0, abstain 0 (3).

MAILING LIST: It was determined that Jennifer Seberry would look into the best way to maintain the mailing list. Jennifer is to have a proposal to the board by CRYPTO '93.

BOD meeting on Wednesday, 26 May to cover the financial update, EC '95 proposal, CRYPTO '94 general chair, IACR bulletin board, Submission by RSA to Newsletter (charge?), Future Strategy.

Adjourn Gordon made a motion to adjourn the meeting. Tom seconded. MEETING ADJOURNED.

MEETING OF BOARD OF DIRECTORS ON WEDNESDAY, 26 May at 12:10 p.m. In attendance were all from above meeting with proxies as stated with the exception of Andy Clark. Agenda was accepted as a continuation of the prior meeting.

FINANCIAL REPORT UPDATE: Peter reported that he had spoken with Kevin. Kevin said that the EC '92 financial report can now be completed as Kevin has received the final information from Rainer Rueppel. Concerning CRYPTO '92, Kevin has spoken with Spyros and things are being finalized. Kevin will prepare for the Newsletter the final and complete financial report. This should be done within two to three weeks.

EUROCRYPT '95: Louis Guillou proposed that EC '95 be held in Saint Malo, France. The conference would take place at the Palais Du Grand Large. A preliminary budget was proposed and will need to be reviewed by Kevin and Peter. The General Chair would be Francois Scanrabin and Program Chair will be Louis.

Tom Berson made a motion that the proposal be accepted. Seconded by Gordon. Vote: For 10; No 0, abstain 0 (3).

CRYPTO '94 GENERAL CHAIR: Several names were discussed and it was by unanimous vote that Jimmy Upton and Stafford Tavares will be asked to chair CRYPTO '94 and CRYPTO '95.

SUBMISSION OF RSA CONFERENCE ANNOUNCEMENT TO NEWSLETTER: After discussion, it was moved by Bob Blakley that the decision of the publication of the Newsletter and its contents be at the discretion of the Newsletter Editor. Ingemar Ingemarsson seconded. Vote: For 9; No 0; Abstain 1 (3).

IACR BULLETIN BOARD: Andy Clark presented his write up on this subject. It was discussed at great length and it was decided that the subject will not be pursued at this time. Peter will report to the General Assembly.

FUTURE STRATEGIES: There was discussion on parallel sessions at the conferences, local chapters of IACR, plans for growth and the proceedings. Peter reported his conversation with Hoffman of Springer concerning the proceedings for EC '93 and the proceedings for Auscrypt '92. Andy submitted a paper for consideration by the Ad Hoc Committee. Yvo brought up the concern about EC and CRYPTO for the year 2000 and what name will be used. Nothing resolved at this time.

CRYPTO '93 BOD MEETING: CRYPTO '93 BOD meeting will be held on Sunday, 22 August at 2:00 at UCSB. Paul to organize meeting place.

GENERAL ASSEMBLY: It was decided what to present to the General Assembly today at 17:10 hrs..

OTHER: The subject of the "Clipper" chip and what the IACR's position is and if a statement will be issued. After much discussion, it was decided that Whit, Tom and Ron will work on wording. A subsequent meeting of the board will take place at 18:00 hrs. for fifteen minutes only. At that time, the board will vote whether to issue a statement or not.

ADJOURNED.

BOD EC '93 Meeting 26 May, 1993 After the General Assembly the Board of Directors met at 18:15 hrs. to discuss the board's statement concerning the "Clipper" chip. The same board members were in attendance as in the two previous meetings.

Ron Rivest presented his draft statement. There was much discussion about this statement. Whitfield Diffie moved for the following resolution:

> *"The Board of Directors of the IACR feels that the recent proposal by the United States to adopt a cryptographic standard incorporating a secret algorithm for the means of government eavesdropping is of major importance to society and lies within the expertise of the IACR and its members. It therefore resolves to take prompt action to inform the membership of the society on these developments."*

Yvo Desmedt seconded the motion. Vote: For 10, No 0; abstain 2 (5).

Concerning the statement by Ron, further discussion followed. It was moved by Sherry McMahan to have a final draft of the statement sent via electronic mail to all board members by the end of next week and a vote to be taken at that time. The motion was seconded by Yvo. Vote: For 12, No 0; abstain 0 (3).

Adjourned.

The following statement was sent via email to all the board members:

> *"The International Association for Cryptologic Research (IACR) is a professional organization devoted to promoting research and development of cryptology for the public welfare.*
>
> *"While the best known application of cryptography is to provide privacy of communications, cryptography is an essential component of the information infrastructure of modern society. Today, cryptography provides capabilities such as pay television, electronic funds transfer, and secure electronic mail. Future applications envisioned include electronic voting, electronic money, and protection of intellectual property rights. Cryptology is an essential tool in the design and implementation of an information based society.*
>
> *"The Board of Directors of the IACR has learned of the recent proposal by the U.S. government to standardize a cryptographic system incorporating a secret enciphering algorithm and a means of government eavesdropping for law enforcement. While the Association has not had time to fully understand and evaluate this proposal, the Board notes that this approach raises many issues of public concern. Furthermore, the Board recommends that sufficient time be allocated for this proposal to receive careful attention and broadbased open review."*

Vote: For 14; No 0; abstain 0:

GENERAL ASSEMBLY OF THE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH AT EUROCRYPT '93

Peter Landrock, the president of IACR, called the assembly to order at 17:15 hrs. on 26 May, 1993 at Lofthus, Norway. Peter presented to Kare Presttun and Tor Helleseth certificates of appreciation for their efforts as General Chair and Program Chair for Eurocrypt '93. Special thanks to Leif Nilsen, the program committee and the authors.

Peter introduced the board of directors.

Gordon Agnew spoke about the 1993 election details to appear in the June 1993 newsletter.

Peter announced the schedules for CRYPTO '93 at UCSB from 22 to 26 August, 1993; Eurocrypt '94 in Perugia, Italy from 10 to 12 May, 1994; CRYPTO '94 at UCSB from 21 to 25 August, 1994; and Eurocrypt '95 at Saint Malo, France in May, 1995 (date to be determined).

Tom Berson gave the report for the Journal of Cryptology (see minutes of BOD meeting).

Ross Anderson spoke about the Computer and Communications Security Review journal and Ueli Maurer mentioned his work as Associate Editor for Cryptology and Complexity for the IEEE Transactions on Information Theory.

Financial report was given (see minutes of BOD meeting).

Peter announced that the proceedings for EC '93 would be provided at no extra charge to the participants. Peter mentioned the discussion by the board about the bulletin board. It was decided by the board to not implement a bulletin board at this time.

Open Issues: Peter mentioned that the board was considering making a statement about the "Clipper" chip. There was much discussion. By a show of hands Peter asked the assembly whether or not it might be appropriate for the board to make a statement. The show of hands for was more than against. The board will meet again after the general assembly to discuss.

Adjourned.

Respectfully submitted,

Sherry S. McMahan Secretary

Treasurer's Report

IACR FINANCIAL SUMMARY

As treasurer of IACR, it is my duty to oversee and manage the finances of IACR. As such, I assist conference organizers in the planning, approve conference budgets, pay the bills, and make recommendations to the Board of Directors and the membership regarding financial matters of the Association. I can report at this time that IACR is financially sound, but far from rich. We have about $100,000 in the bank, which gives us a slight cushion against financial disaster.

The only significant income to IACR is through membership fees and any unplanned surplus remaining from our conferences. Most recent conferences have returned a "surplus" that is only enough to cover the cost of purchasing and mailing conference proceedings. During 1992, there were two developments that had significant influence on the financial condition of the IACR. The first of these was the decision by the Board of Directors to increase the number of issues published each year by the Journal of Cryptology, which brought with it a sizeable increase in the cost of subscriptions. The second was the renegotiation of the agreement by which conference proceedings are provided to members. As a result of these developments, I recommended that the dues for IACR be increased from $40 to $50 in 1993, and I warned that further increases will likely be required to account for the increased costs of publications.

A complete picture of the financial condition of IACR would require more space than we have here. So that members may understand the ways that their conference fees are spent, I have provided below a summary of the flow of money for income and expenses (in U.S. dollars).

	Eurocrypt 92	Crypto 92
CONFERENCE INCOME		
registration fees	80100.00	44118.00
room and board	0.00	46145.00
other	700.00	4381.78
(-membership)	<8780.00>	<6300.00>
TOTAL INCOME	72020.00	88344.78
CONFERENCE EXPENSES		
room and board		44968.07
Publicity/mail	4578.00	3246.84
Org/lcl arrngmnts	10201.00	4134.77
meeting facility	9401.00	3756.75
reception/banquet	17804.00	16446.41
lunches (4 for 280)	11477.00	
program committee	2000.00	1523.19
invited lecturers		1525.52
travel assistance		2132.00
preproceedings	4280.00	4732.99

other	689.00	1711.75
TOTAL EXPENSE	60430.00	84178.29
PAID TO IACR		
membership	8780.00	6300.00
residual	11590.00	4166.49
TOTAL	20370.00	10466.49

Expenses in 1992 for IACR (funded by dues) can be broken down as follows:

Legal and Professional fees	$1,230.00
Journal of Cryptology	$12,851.99
Newsletter	$3,935.17
Bank fees	$70.00
Office expenses (bank,postage)	$341.22

Note that the bill that I received this year for Volume 5 of the Journal was $18,690; substantially larger than the previous year. The total assets of IACR as of December 31, 1992 are $132,114.00. Liabilities ran to approximately $28,200, giving a net worth of approximately $104,000. This represents an increase of a few hundred dollars over the previous year. If anyone wishes to receive more detailed information regarding IACR finances, or to make suggestions for future changes in the way IACR runs their conferences or publications, I encourage members to make their suggestions known to me or another officer or director.

Kevin McCurley IACR Treasurer

CRYPTO '93

Conference Announcement & Final 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 (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.

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, 1993. **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 Bell Labs), R. Impagliazzo (UCSD), A. Odlyzko (AT&T Bell Labs), 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
Bell-Northern Research (MAIL STOP 000)
3500 Carling Ave.
Nepean, Ontario K2H 8E9 Canada
Telephone: (613)-763-4199
Fax: (613)-763-2626
Internet: `crypto93@bnr.ca`

CRYPTO '93

GENERAL INFORMATION

August 22 - 26, 1993

The program: Crypto'93 is the thirteenth in a series of workshops on cryptology held at Santa Barbara, and is sponsored by the International Association for Cryptologic Research, 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 (a subsidiary of Northern Telecom). The program for the workshop will cover all aspects of cryptology. Extended abstracts of the papers presented at the conference will be distributed to all attendees at the conference, and formal proceedings will be published at a later date.

In addition to the regular program of papers selected or invited by the program committee, there will be a rump session on Tuesday evening for informal presentations. Facilities will also be provided for attendees to demonstrate hardware, software and other items of cryptographic interest. If you wish to demonstrate such items, you are urged to contact the General Chair so that your needs will be attended to. The social program will include hosted cocktail parties on Sunday and Monday. In addition, there will be a beach barbecue on Wednesday evening. The price of the barbecue is included in the room and board charge, and extra tickets may be purchased.

About the conference facilities: The workshop will be held on the campus of the University of California, Santa Barbara. The campus is located adjacent to the Santa Barbara airport and the Pacific Ocean. Accommodations are available in the university dormitories at relatively low cost for conference participants. Children under the age of 13 are not allowed to stay in the dormitories, so those bringing small children will need to make separate arrangements in one of several nearby hotels. More information on hotels is enclosed. Parking on campus is available at no cost to the participants. However, participants must indicate on the registration form if they desire a parking permit.

Travel information: The campus is located approximately 2 miles from the Santa Barbara airport, which is served by several airlines, including American, America West, Delta, United, and US Air. Free shuttle bus service will be provided between the Santa Barbara airport and the campus on Sunday and Thursday afternoons. All major rental car agencies are also represented in Santa Barbara, and AMTRAK has rail connections to San Francisco from the north and Los Angeles from the south. Santa Barbara is approximately 100 miles north of Los Angeles airport, and 350 miles south of San Francisco.

Registration: Participation is invited by interested parties, but attendance at the workshop is limited, and pre-registration is strongly advised. Late registrations, subject to a late registration fee, may be accepted if space is available, but there are no guarantees. To register, fill out the attached registration form and return to the address on the form along with payment in full before July 9, 1993. Campus accommodations will be available on a first come, first serve basis for attendees who register by July 9, 1993. The conference fees include participation in the program and all social functions, as well as membership to the IACR and a subscription to the Journal of Cryptology. The room and board charges include dormitory lodging and meals from dinner on Sunday to lunch on Thursday. Technical sessions will run from Monday morning to Thursday at noon. A very limited number of stipends are available to those unable to obtain funding. Applications for stipends should be sent to the General Chair before June 4, 1993.

CRYPTO '93 Registration Form

Registration deadline: July 9, 1993

Last Name: ____

First Name: ______________________________ Sex: (M)__ (F)__

Affiliation: ____

Mailing Address: ____

____

____

____

Phone: ______________________ FAX: ______________________

Electronic Mail: ____

Payment of the conference fee entitles you to membership in the International Association for Cryptologic Research for one year at no extra charge, including a subscription to the Journal of Cryptology, published by Springer-Verlag, at no extra charge. Do you wish to be an IACR member? YES__ NO__

The conference fee also includes the conference proceedings when they become available, containing final versions of conference papers. The book of extended abstracts distributed at the conference will contain only shortened preliminary versions of these papers (maximum 10 pages).

Conference fee: Regular ($280) US$______

Attended Eurocrypt'93, Norway ($230) ______

Full time student ($190) ______

deduct $50 if you do not wish the proceedings ______

Total conference fee: US$______

Room and Board (4 nights): Smoking ____ Non-smoking ____

Single room ($275 per person) ______

Double room ($225 per person) ______

Roommate's name: ______________________________

Extra barbecue tickets ($20 each; one is included in the room and board charge) ______

$40 late fee for registration after July 9; ***registration not guaranteed after July 9*** ______

Total funds enclosed (U.S. dollars): US$ ______

Payment must be by check payable in U.S. funds, by money order in U.S. funds or by U.S. bank draft, PAYABLE TO: CRYPTO'93. Payment should be mailed to the General Chair:

Paul C. Van Oorschot, CRYPTO'93
Bell-Northern Research (MAIL STOP 000)
3500 Carling Ave.
Nepean, Ontario
K2H 8E9 Canada

Hotels

For those who choose not to stay in the dormitories, the following is a partial list of hotels in the area. Those who choose to stay off campus are responsible for making their own reservations, and early reservations are advised since August is a popular season in Santa Barbara. Note that Goleta is closer to UCSB than Santa Barbara, but that a car will probably be required to travel between any hotel and the campus. All prices are subject to change; prices should be confirmed by calling the individual hotels directly. However, mention *CRYPTO'93* when you are making your reservation and in several of the hotels listed you will be eligible for the **university rate** which can be significantly less than the normal rates. We are not able to block rooms in these hotels, so please make reservations as early as possible. The quality of the hotels range from rather expensive beach-front resorts to basic inexpensive accommodations. For further information, try contacting the Santa Barbara Convention and Visitors Center, (805)-966-9222.

South Coast Inn: 5620 Calle Real, Goleta, CA 93117. Regular rates: Single $89, Double $94; call for University rates. Contact Murrill Forrester at (805)-967-3200 or toll-free at (800)-350-3614.

Cathedral Oaks Lodge: 4770 Calle Real, Santa Barbara, 93110. Single rates not available, Double rates start at $84 including breakfast; no University rates. Call Tom Patton at (805)-964-3511 or toll-free at (800)-654-1965.

Motel 6: 5897 Calle Real, Goleta, CA 93117. Single $33.95, Double $39.95, no University rate available. Call (505)-891-6161.

The Sandman Inn: 3714 State St., Santa Barbara, CA 93105. Regular rates: Single or Double $84, $94 for king-size, University rate $65. Call Jean Ingerle at (805)-687-2468 or toll-free at (800)-350-8174.

Miramar Hotel (Beachfront): 3 miles south of Santa Barbara on U.S. 101 at San Ysidro turnoff. Regular rates: $70-$135. No University rates. Call (805)-969-2203.

Pepper Tree Inn: 3850 State St., Santa Barbara, CA 93105. Regular rates: $106-$112 for two people, University rates $96-$102 for two people. Call Christopher Oliphant at (805)-687-5511 or toll-free at (800)-338-0030.

Encina Lodge: 220 Bath Street, Santa Barbara, CA 93105. Regular rates $106-$108 for two people, no University rates. Call Carol Wolford at (805)-682-7550 or toll-free at (800)-526-2282.

Quality Suites: 5500 Hollister Ave, Santa Barbara, CA 93111 (close to campus). Regular rates: Single $125, Double $145, University rates $99 double (must mention you are attending a UCSB program). Call Michael Ensign at (805)-683-6722.

Upham Hotel (bed-and-breakfast): 1404 De La Vina Road, Santa Barbara, CA 93101. University rate $85 (mention you are from Crypto). Call Sheila Donegan at (805)-962-0058.

Conference Announcements

ADVANCED SCHOOL ON COMPUTATIONAL LEARNING AND CRYPTOGRAPHY

Vietri sul Mare (Italy), September 13-24, 1993

Sponsored by the Italian Chapter of the EATCS Aims and Scope

Learning and cryptography are becoming more and more important in computer science and its applications, and recent theoretical developments showed that they have interesting points of contact. The importance of Cryptography has been recognized for centuries. With the recent advances in communication and computer technology, a vast amount of financial and commercial information are stored and transferred on computer networks. This has motivated an enormous amount of activity in the field of Cryptography in the past two decades. This period has been marked by the introduction of several revolutionary new concepts such as public-key cryptography, zero-knowledge proofs systems, and provably secure protocols. Complexity theory and computational number theory have provided the conceptual tools for this exciting area of computer science. Learning is emerging as a computational paradigm alternative to explicit programming, since in many cases it appears much easier to "train" a machine to perform a given task, or to recognize a given set of objects, by showing a set of examples rather than by writing a programs which explicitly covers all the possible situations. As for cryptography, the practical relevance of learning has stimulated theoretical research on learning from examples, giving rise to a very active area known as Computational Learning Theory. Different formal models of learning from examples, which take into account computational complexity aspects of learning, in the line of Valiant's Probably Approximately Correct (PAC) learning model, have been defined and compared, and classes of concepts learnable within polynomial resource bounds have been characterized, using in some cases cryptographic lower bound techniques. The objective of the Advanced School is to present some recently developed formal methods and techniques in these two areas of theoretical computer science. The fascinating relationships between cryptography, learning and complexity theory will been unfolded. Furthermore, it will be discussed how this kind of theoretical concepts relates to a topic of applicative interest such as learning in neural networks.

Directors

Prof. Alfredo De Santis, Universita' di Salerno Prof. Giancarlo Mauri, Universita' di Milano

Lecturers

Prof. Shimon Even, Technion, Haifa, Israel
Dr. Moti Yung, IBM Watson Ctr., Yorktown Heights, New York, USA
Dr. Michael Kearns, AT&T Bell Labs, Murray Hill, New Jersey, USA
Prof. Wolfgang Maass, Technische Universitaet Graz, Austria

Venue

The Advanced School will take place at the IIASS Center in Vietri sul Mare, near Salerno and Neaples (Italy)

Organization

The Advanced School is organized by the Italian Chapter of the European Association for Theoretical Computer Science, and with the support of the Universities of Milano and Salerno and of the CNR. A number of about 40 students of any nationality will be selected for admission. The school will consist of four courses (10 hours each) and of short seminars given by participants and other invited speakers. Monday, September 13th, will be dedicated to arrivals. Two courses will be allocated in the four days from Tuesday, September 14th, to Friday, September 17th. The remaining courses will be taught in the first four days of the second week, i.e. from Monday September 20th to Thursday, September 23th. Saturday, September 18th, and Friday, September 24th, will be dedicated to short seminars.

Applications

PhD students in Computer Science as well as researchers and Teachers in the field are invited to apply for participation. Applicants should fill in the attached application form and return it together with a Letter of recommendation of their Department or Institution as soon as possible, and in any case before June 15th, 1993, to:

Prof. Alfredo De Santis
Dip. di Informatica e Applicazioni
Universita' di Salerno
84081 Baronissi (SA)
Italy
Tel. +39 89 822329
Fax +39 89 822272
e-mail: ads@udsab.dia.unisa.it

The applications will be considered with due regard to a fair distribution of available places among applicants from the various countries. The number of participants will be limited to 40. All applicants will receive notice by July 10th, 1991.

Living expenses and Participation fee

Participants will be accommodated in hotels nearby the IIASS. One day of full board prices for one participant costs about as follows (prices are in Italian Lire):

	Hotel Vietri	Hotel La Lucertola Hotel Bristol
double room-per person	55.000	75.000
single room	60.000	95.000

The participation fee amounts to Italian Lire 500.000. Graduate Students are not requested to pay the participation fee. Limited funds are available for those participants who will need financial aid to cover a part of their costs.

Very Important

Please fill in your application form properly and completely. An application without a Letter of Recommendation will not be taken into consideration.

I hereby apply for admission as participant in the Advanced School on Computational Learning and Cryptography, Vietri sul Mare, Italy, September 13-24, 1993.

Surname: ______________________________

First name: ______________________________

Date of birth: ____________________ Sex: ________

Nationality: ______________________________

Address: ______________________________

____

Phone number: ______________________________

Fax number: ______________________________

E-mail address: ______________________________

Professional position: ______________________________

Current interests in computer science: ____________________

____

Recent publications (no more than 5): ____________________

____

____

____

____

____

Do you want to pass an examination at the Advanced School ? _____

Do you want to give a Seminar at the Advanced School ? (if yes,

enclose a title and a short summary (200 words)____________

Date: ______________________________

Signature: ______________________________

For Graduate Students only:

I declare that I am currently a Graduate Student at the: ________

____

Signature ______________________________

Enclosures:

A letter of recommendation from: ____________________

____

The Workshop on Information Protection

CONFERENCE ANNOUNCEMENT

The Workshop on Information Protection, organized by the Institute for Problems of Information Transmission of Russian Academy of Sciences with Russian Chapter of the Information Theory Society IEEE, will be held in Moscow on **December 6-9, 1993**. The conference program will include invited lectures and 20 min. talks. The following sessions are planned:

- Cryptography and authentication
- Error-correcting coding
- Coded modulation

CLIMATE

Average temperatures at the beginning of December are about -5° C during daytime.

ACCOMMODATION and TRANSPORT

The Conference Organization will provide good boarding-house and hotel accommodations at reasonable prices. Conference will take place in the suburb of Moscow. The bus and car service will be provided.

INSTRUCTIONS for AUTHORS

Authors of talks are requested to send an abstract (not more than 300 words) to the Program Chair at the address given below. Sending a LaTeX style file by e-mail is strongly recommended. The full texts of lectures and talks are expected to be published after the Workshop.

CONFERENCE FEE

Conference fee is 150 USD (cash is preferable) and includes the following:

- Participation in the scientific program
- One copy of the pre-proceedings
- Coffee break service
- Conference banquet
- Participation in the cultural program
- Transport service.

IMPORTANT DATES

The first deadline for registration will be **September 15, 1993**. The deadline for submission of abstracts will be **October 1, 1993**.

ORGANIZING COMMITTEE

Victor V.Zyablov (Chairman, IPIT, Russia), Andrew L.Chmora (Scientific secretary, IPIT, Russia, chmora@ippi.msk.su), Natalia V.Ikoeva (IPIT, Russia), Gregory A.Kabatianskii (IPIT, Russia), Nikolay A.Kuznetsov (IPIT, Russia), Vladimir K.Levin (KVANT, Russia) Vladimir I.Venets (IPIT, Russia).

PROGRAM COMMITTEE

Ernst M.Gabidulin (Chairman, MIPT, Russia, gab@ippi.msk.su), Valentin B.Afanasiev (IPIT, Russia), Leonid A.Bassalygo (IPIT, Russia), Thomas Berson (Anagram Lab., USA), Gerard Cohen (ENST, Paris, France), Martin Hellman (Stanford University, USA) Rolf Johannesson (Lund University, Sweden), Vladimir M.Sidelnikov (Moscow State University, Russia), Claus Schnorr (Universitat Frankfurt, Germany).

FURTHER INFORMATION

For further information, please contact

Victor V.Zyablov
Russian Academy of Sciences
Institute for Problems of Information Transmission
19 Yermolovoy St. Moscow 101447 GSP-4 Russia
Telephone: (095)-299-5096
Fax: (07)-(095)-209-0579
E-mail: zyablov@ippi.msk.su

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

PERUGIA

EUROCRYPT '94

May 10 - 12, 1994

University of Perugia, Italy

A Workshop on the Theory and Applications
of Cryptographic Techniques

Sponsored by
the International Association for Cryptologic Research (IACR)

CONFERENCE ANNOUNCEMENT

Eurocrypt '94 continues the tradition of European IACR conferences dedicated to the theory and applications of cryptographic techniques. Most areas of theoretical and practical cryptography will be considered in the "Call for papers", to present an in depth survey and to explore current and future developments affecting the confidentiality and the integrity of information.

Eurocrypt '94 will be held at the "Aula Magna" of the University of Perugia.
Perugia, which was an historical Etruscan capital, is not only an important centre of industry, commerce and handicrafts, but also the seat of cultural and teaching institutes, some of which are very ancient as the University dated 1266, while others are more recent, but equally renowned, as the Italian University for Foreigners.
Perugia, famous in the centuries for the incomparable beauty of its architecture and sculpture, in the Renaissance enriched the world by its mystical, gentle school of painting (Bartolomeo Caporali, Perugino, Pinturicchio, Raffaello).

TRANSPORT

Perugia can be reached by plane via Milano (456 km) and either by train or bus from Roma (170 km). Furthermore a bus service from Roma to Perugia could be arranged by the Conference Organizers on May 9, if a sufficient number of people will request it.

CLIMATE

Average temperatures in May usually are 20-25 °C during daytime.

ACCOMODATION

The Conference Organization will provide good hotel accomodations at reasonable prices. Further information will be given in the next announcement.

IMPORTANT DATES

The first deadline for registration will be **April 1, 1994.**
The deadline for submission of extended abstracts will be **January 10, 1994.** Send 12 copies of an extended abstract of at most 10 double spaced pages to the Program Chairman.
Additional information and a "Final call for papers" will be sent to the attendees of previous Eurocrypt and Crypto conferences around September 1, 1993. For further information and to make sure you are on the mailing list, write to the conference address.

GENERAL CHAIRMAN

William Wolfowicz
Fondazione Ugo Bordoni
Via Baldassarre Castiglione 59
00142 ROMA RM
Italy

ph.: +39 6 54803330
fax: +39 6 54804403
E-mail: cripto @ itcaspur.bitnet

PROGRAM CHAIRMAN

Alfredo De Santis
Università di Salerno
Dip. Informatica e Applicazioni
84081 BARONISSI SA
Italy

ph.: +39 89 822329
fax: +39 89 822272
E-mail: ads @ udsab.dia.unisa.it

ORGANIZING COMMITTEE

William Wolfowicz (Fondazione Ugo Bordoni, FUB)
Franco Bertoldi (Istituto Internazionale delle Comunicazioni, IIC)
Saverio Cacopardi (Università di Perugia)
Michele Elia (Politecnico di Torino)
Giuseppe M. Poscetti (Università di Roma "La Sapienza")
Andrea Sgarro (Università di Trieste)

CONFERENCE SECRETARIAT

Istituto Internazionale delle Comunicazioni, IIC
Eurocrypt '94 Secretariat
Via Pertinace, Villa Piaggio
16125 GENOVA GE
Italy

ph.: +39 10 2722383
fax: +39 10 2722183

Transitions

Andrew Klapper
Dept. of Computer Science
915 Patterson Office Tower
University of Kentucky
Lexington, KY 40506-0027
USA

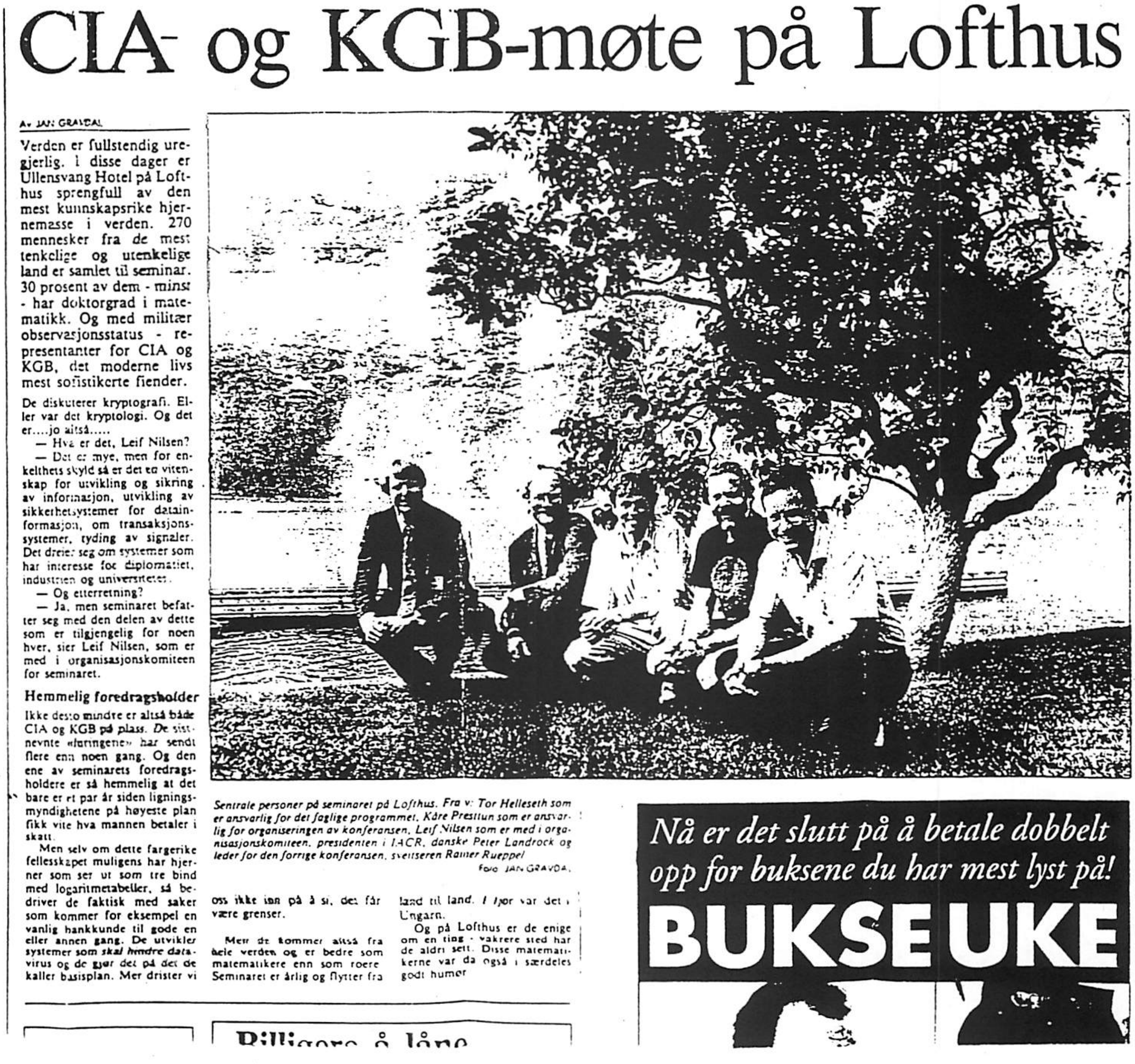
e-mail: klapper@ms.uky.edu

Recent Thesis and Reports

"Risk Analysis in Computer Networks", Zan Anastovski, Centre for Computer Security Research, University of Wollongong, Wollongong, NSW 2522 - Australia.

Late Breaking News

Headlines in the local paper in Lofthus (obviously they know something we don't!). *"CIA and KGB meet in Lofthus"*



CIA- og KGB-møte på Lofthus

Av JAN GRAVDAL

Verden er fullstendig uregjerlig. I disse dager er Ullensvang Hotel på Lofthus sprengfull av den mest kunnskapsrike hjernemasse i verden. 270 mennesker fra de mest tenkelige og utenkelige land er samlet til seminar. 30 prosent av dem - minst - har doktorgrad i matematikk. Og med militær observasjonsstatus - representanter for CIA og KGB, det moderne livs mest sofistikerte fiender.

De diskuterer kryptografi. Eller var det kryptologi. Og det er....jo altså.....

— Hva er det, Leif Nilsen?

— Det er mye, men for enkelthets skyld så er det en vitenskap for utvikling og sikring av informasjon, utvikling av sikkerhetsystemer for datainformasjon, om transaksjonssystemer, tyding av signaler. Det dreier seg om systemer som har interesse for diplomatiet, industrien og universitetet.

— Og etterretning?

— Ja, men seminaret befatter seg med den delen av dette som er tilgjengelig for noen hver, sier Leif Nilsen, som er med i organisasjonskomiteen for seminaret.

Hemmelig foredragsholder

Ikke desto mindre er altså både CIA og KGB på plass. De sistnevnte «luringene» har sendt flere enn noen gang. Og den ene av seminarets foredragsholdere er så hemmelig at det bare er et par år siden ligningsmyndighetene på høyeste plan fikk vite hva mannen betaler i skatt.

Men selv om dette fargerike fellesskapet muligens har hjerner som ser ut som tre bind med logaritmetabeller, så bedriver de faktisk med saker som kommer for eksempel en vanlig bankkunde til gode en eller annen gang. De utvikler systemer som *skal hindre datavirus* og de gjør det på det de kaller basisplan. Mer drister vi oss ikke inn på å si, det får være grenser.

Men de kommer altså fra hele verden og er bedre som matematikere enn som roere. Seminaret er årlig og flytter fra land til land. *I fjor* var det i Ungarn.

Og på Lofthus er de enige om en ting - vakrere sted har de aldri sett. Disse matematikerne var da også i særdeles godt humør

Sentrale personer på seminaret på Lofthus. Fra v: Tor Helleseth som er ansvarlig for det faglige programmet, Kåre Presttun som er ansvarlig for organiseringen av konferansen, Leif Nilsen som er med i organisasjonskomiteen, presidenten i IACR, danske Peter Landrock og leder for den forrige konferansen, sveitseren Rainer Rueppel

Foto JAN GRAVDAL

Billigere å låne