IACR

NEWSLETTER

A Publication of the International Association for Cryptologic Research

Volume 11 Number 1 January 1994

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
William Wolfowicz
Fondazione Ugo Bordoni, FUB
Via Baldassarre Castiglione, 59
00142 ROMA RM
Italy
cripto@itcaspur.bitnet
+39 6 54803330
+39 6 54804403 Fax

Crypto 93 Chair
Jimmy R. Upton
Uptronics Incorporated
1590 Oakland Road
Suite B203
San Jose, CA 95131
USA
jupton@netcom.com
+1 (408) 451 8901 fax

Newsletter Editor
Gordon B. Agnew
Dept. of Electrical Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada
gbagnew@crypto1.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

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

Rainer Rueppel[4]
R^3 Security Engineering AG
Zürichstrasse 151
CH-8607 Aathal
Switzerland
+41 1 932 6660

Jennifer Seberry[4]
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[4]
Dept. of C&O
Univ. of Waterloo
Waterloo, Ontario, Canada
N2L 3G1
savansto@math.uwaterloo.ca
1 519 885 1211 X4036

[1] Term expires Dec. 1995

[2] Term expires Dec. 1994

[3] Term expires Dec. 1995

[4] Term expires Dec. 1996

EDITOR'S CORNER

Greetings and Happy New Year from the frozen North! There are many things happening in the world of the IACR.

First, we have election results to report on (see the next page). I would like to congratulate all of the returning officers and directors as well as welcome the new directors. I would like to take this opportunity on behalf of the IACR to thank Ron Rivest and Yvo Desmedt for all of their contributions to the IACR.

As some of you know, the IACR is still suffering from growing pains. In the past, much of our activities were handled in a very informal manner. Our progressive growth has necessitated the formalization of many of our procedures. Unfortunately, sometimes, things fall between the cracks. During the past election, some members of IACR did not receive their election ballots in the first mailing. This was the result of a small glitch in the mailing label generation program. We managed to correct the problem in a second mailing of ballots. This unfortunately delayed the counting of ballots and made the Returning Officer's job that much more difficult. I would like to thank Andy Clark for his tireless efforts in getting the ballots counted and results returned. I would also like to thank Tom Berson for his efforts on the noinations and election committee. As I mentioned before, we are implementing new procedures and plans are underway to formalize the way in which nominations and elections (especially the mailing labels) are handled.

Other news includes the very successful CRYPTO'93 conference. I would like to congratulate Paul on a very well run conference and thank
him for his efforts.

ELECTION RESULTS

As Returning Officer for the above election and on behalf of the Nominations Committee I hereby present the results of the IACR Election 1993.

1. TWO candidates stood for the position of President, voting was as follows:

Peter Landrock	117
Jennifer Seberry	44

Peter LANDROCK is elected President

2. ONE candidate stood for the position of Vice President, voting was as follows:

Ingemar Ingemarsson	141

Ingemar INGEMARSSON is elected Vice President

3. ONE candidate stood for the position of Secretary, voting was as follows:

Sherry McMahan	146

Sherry MCMAHAN is elected Secretary

4. ONE candidate stood for the position of Treasurer, voting was as follows:

Kevin McCurley	148

Kevin MCCURLEY is elected Treasurer

5. NINE candidates stood for the position of Director, voting was as follows:

Walter Fumy	40
Richard Graveman	22
Spyros Magliveras	15
Rainer Rueppel	100
Jennifer Seberry	73
Stafford Tavares	30
Paul Van Oorschot	66
Scott Vanstove	84
Johan van Tilburg	33

Rainer RUEPPEL, Jennifer SEBERRY and Scott VANSTONE are elected Directors.

I declare that the above information is true and correct.

Notes: =====

a) 157 Members voted

b) There were 20 further submissions which were spoiled and hence did not count towards the result

c) I shall be writing to all candidates formally telling them of their success/failure in the election. I expect to send those letters within the next week.

By copy of this email I request that Gord Agnew publish these results in the January newsletter.

Respectfully submitted - Andrew J Clark, Returning Officer, 9 December 1993

IACR BOARD OF DIRECTORS MEETING CRYPTO '93

The Board of Directors Meeting of the International Association for Cryptologic Research was called to order at approximately 2:00 p.m. by the President, Peter Landrock, on 22 August prior to the Crypto '93 at UCSB in Santa Barbara, CA. In attendance were the following officers - Peter Landrock, Kevin McCurley (arrived late), Ingemar Ingemarsson and Sherry McMahan; directors - Tom Berson, Andy Clark, Scott Vanstone, Jean-Jacques Quisquater, Bob Blakley, Ron Rivest, Whit Diffie (arrived late), Paul Van Oorschot, Yvo Desmedt, Hideki Imai and Gilles Brassard (arrived late). Also in attendance were Jimmy Upton and Jennifer Seberry. Absent were Gordon Agnew (Tom Berson has Gordon's proxy, which is counted as an abstention unless specifically voted) and Kare Presttun.

The AGENDA was modified to include setting the date for Crypto '95, appointment of program chair for Crypto '94 and the issue of honors. Scott moved that the modified agenda be accepted, seconded by Ingemar. Vote: For - 11; Against - 0; Abstain - 1.

EUROCRYPT '94 REPORT: Reported by Peter - Eurocrypt '94 will be held from 9 to 12 May, 1994 in Perugia, Italy. William Wolfowicz has submitted a budget to Kevin and Peter for review. This will be reviewed and any necessary modifications will be made. Alfredo De Santis is the Program Chair and the call for papers has been made, deadline for submissions for the conference is 10 January, 1994.

EUROCRYPT '93 REPORT: Kare Presttun sent a status report of the financial situation to Peter and Kevin. It appears that the conference will have the funds to cover the cost of the proceedings with a small surplus to be returned to the IACR.

CRYPTO '93 UPDATE: Paul reported that he expects approximately 250 attendees and that it appears that the conference will come in under budget.

JOURNAL OF CRYPTOLOGY: Gilles reported that all is on schedule for Volumes 6 and 7. Gilles recommended that the Journal remain at 4 issues per volume with two 64 page issues and two 48 page issues. It was moved that this recommendation be accepted. Vote: For - 13; Against - 0; Abstain - 1.

Gilles appointment as editor will end on 31 December, 1993. It was moved that 1) Gilles appointment be extended for one year, 2) that the board enter into a non binding agreement for the 1994 and 1995 Board of Directors to extend Gilles appointment as editor for two more one year extension (or until the Bylaws have been revised to allow extensions of up to three years) and 3) that the Committee reviewing the Bylaws modify the Bylaws to allow extensions for the Journal Editor for up to three years at a time and that the Editor can be reappointed. The motion was seconded. Vote: For - 13; Against - 0; Abstain - 1.

FINANCIAL REPORT: Kevin presented the Financial Summary for 1992. The tax forms for 1992 have been submitted to the IRS. As decided by the Board at Eurocrypt '93, Kevin will commit approximately 1/2 of the IACR funds to Certificates of Deposits with the balance remaining in an interest bearing checking account.

The IACR is incorporated in the state of Nevada and a resident agent files forms for the IACR to the State of Nevada. Because of certain misgivings about the current resident agent, it was moved that Tom Berson will find a new resident agent for the IACR. Vote: For - 14; Against - 0; Abstain - 1.

Kevin also recommended that the General Chair Guidelines include a recommendation that all conferences have indemnity insurance. (Note: it is a requirement that Crypto have insurance.) It was also recommended that the nominating committee include on future nomination forms the fact that a member of the Board of Directors of IACR is a member of the Board of a 501(c)(3) (non profit) organization that is incorporated in the State of Nevada. These recommendations were noted by the individuals involved in the respective committees.

COMMITTEE REPORTS:
Report by Yvo on the review of the Program Committee Guidelines- Yvo has sent to the board his suggested changes and these were reviewed. The name should be changed to "Program Chairman Guidelines and Principles". It was moved that Yvo revise the guidelines and send a copy to each board member by email. Vote: For - 14, Against - 0; Abstain - 1.

General Chair Guidelines - Jennifer has received the guidelines via email and has also received comments from board members and others. She will revise the Guidelines, revise the title to be "General Chairman Guidelines and Principles" and send out copies before the Board of Directors meeting at Eurocrypt '94.

Bylaws Committee: Peter, Ingemar and Sherry mentioned possible changes to the Bylaws. It was moved that the Bylaws be revised and distributed for review by the Board. Objective is to have the vote on the new Bylaws at the Board of Directors meeting at Eurocrypt '94 and then for a ballot to be sent to all the membership. Vote: For - 14; Against - 0; Abstain - 1.

Committee Proceedings: Tom Berson presented a report on the proceedings (copy available on request). It was moved to adopt the proposal that proceedings will presented at the conference, if possible for Eurocrypt '94 and most certainly for Crypto '94. Vote: For - 13; against - 0; Abstain - 2. It was also moved to create instructions to the Author on how to prepare the papers. Vote: For - 13; Against - 0; Abstain - 2. Kevin and Scott volunteered to prepare the instructions and have them to the Program Chair for Eurocrypt '94 and Crypto '94 by January, 1994 Peter to send, before Crypto ends, an email to Alfredo De Santis concerning this issue. (Note: Peter was unable to reach Alfredo during the conference and since the call for papers for Eurocrypt '94 has been sent out, it was decided to have Crypto '94 be the first with proceedings presented at the conference.)

PROGRAM CHAIR FOR CRYPTO '94: Two names were put forward and these will be discussed during the continuation of the board meeting at 12:00 noon on 23 August.

Meeting Adjourned at approximately 5:30 p.m..

RECONVENED MEETING:

Meeting for the Board of Directors was reconvened at around 12:25 p.m. on 23 August. Same attendees (and proxy) at prior meeting except for Paul who could not attend.

EUROCRYPT '95 REPORT: Jean-Jacques reported that Eurocrypt '95 will be held from 22 to 25 May, 1995 in Saint Malo, France. Ms. Scanrabin of CCETT will be the General Chair and Louis Guillou will be the Program Chair.

ASIACRYPT '94: Jennifer reported that Asiacrypt '94 will be held from 28 November to 1 December, 1994 in Wollongong, NSW, Australia. Jennifer is the General Chair and Josef Pieprzyk is the Program Chair.

Peter will send a letter to Jennifer on behalf of the IACR to clarify the issues of "in cooperation with", IACR membership fee of $50 to be paid in US dollars to the IACR, and instructions on the use of the IACR membership and mailing lists.

CRYPTO '95: - Kevin will send to Sherry a copy of the suggested dates proposed to UCSB several years ago by Tom Berson. These includes dates for Crypto up to year 2000. After Jimmy Upton has received the suggested dates from Kevin and/or Sherry he will confirm with UCSB. Stafford Tavares will be the General Chairman of Crypto '95. Program Chairman will be decided at Crypto '94.

PROCEEDINGS OF CRYPTO '92: Ernie Brickell came in to report that all has been submitted to Springer and that he has the Table of Contents to pass out to those interested.

COMMITTEE REPORT (continued):
Nomination Committee - Tom Berson presented the suggested Guidelines prepared by Gordon. A vote was taken on write in candidates on the ballots. Vote: For - 3; Against - 8; abstain - 2. All comments should be sent to Gordon via email and he will prepare with revisions and submit a copy to the Secretary for archival purposes.

As returning officer for this year's election, Andy Clark asked the board to allow him to find two independent witnesses instead of two IACR members to attest to the election results. The board agreed unanimously to allow this.

IACR SEAL: Kevin had received the seal but it was for the AACR instead of IACR. Kevin is to request new seal and the President will hold the seal. It was agreed that Peter should prepare letterhead for the IACR President.

HONORS: Peter appointed an ad hoc committee to review the idea of honors. The committee includes Bob, Yvo and Whit. This committee is to present a report and recommendation to the Board of Directors at the Eurocrypt '94 meeting. Peter to ask David Naccache to resubmit his proposal from Gemplus to provide smart cards.

UCSB CREDENTIALS: It was moved to have 1 faculty and 2 students from UCSB be provided attendance to the Crypto conference and 1 copy of the proceeding. Vote: For - 13: Against - 0; Abstain - 1.

PROGRAM CHAIRMAN FOR CRYPTO '94: Yvo Desmedt was unanimously voted as Program Chairman for Crypto '94.

OTHER BUSINESS: Date for Eurocrypt '94 IACR Board of Directors meeting is on Monday, 9 May, 1994. Time and place to be determined.

Meeting Adjourned.

Respectfully submitted,
Sherry S. McMahan
IACR Secretary

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

Peter Landrock, the president of IACR, called the General Assembly to order at 4:05 p.m. on 25 August at Santa Barbara, CA. Peter introduced the Officers and the Directors. Peter presented certificates of appreciation to Paul Van Oorschot and Doug Stinson for the great job of organizing Crypto '93.

Peter announced the schedules for 1994 and 1995 conferences: Eurocrypt '94 in Perugia, Italy from 9 to 12 May, 1994; Crypto '94 in Santa Barbara from 21 to 25 August, 1994; Eurocrypt '95 in Saint Malo, France from 22 to 25 May, 1995; and Crypto '95 in Santa Barbara, CA from 27 to 31 August, 1995.

CRYPTO '94: Jimmy Upton is the General Chair (email jupton@netcom.com) and Program Chair is Yvo Desmedt (email desmedt@cs.uwm.ed.) Jimmy announced that there will be Saturday accommodations available in the dorms at UCSB if any one is interested and also he is considering combining dinner and the cocktail party on Sunday and Monday nights. Email addresses will be added to the list of the attendees. Any other suggestions or comments, contact Jimmy at his email address.

ASSOCIATED CONFERENCES ("in cooperation with IACR"): Jennifer Seberry announced that Asiacrypt '94 will be held in Wollongong, NSW, Australia (50 miles south of Sydney) from 28 November to 1 December, 1994. This conference is being held the week following the IEEE conference in Sydney. Jennifer is the General Chairman and Josef Pieprzyk is the Program Chairman.

NOMINATION AND ELECTION COMMITTEE: Andrew Clark spoke about the Elections to be held this year. The elections are for the four officer positions and three directors positions. Nominations will close on 15 September, 1993 and ballots will be mailed by 1 October, 1993. Ballots must be mailed to be received by the Returning Officer in the official envelopes by 15 November, 1993. Gordon Agnew is the chair of the Nomination and Election Committee, Tom Berson is a member and Andrew Clark is a member and returning officer.

FINANCIAL REPORT: Kevin McCurley gave the financial report (see report from minutes of Board of Directors meeting).

JOURNAL OF CRYPTOLOGY: Gilles Brassard gave the report on the Journal. All is going well. Volume 6, Issue 2 has been mailed and Volume 6, Issue 3 is being printed. Springer is now printing the Journal in the U.S. instead of Germany. Gilles announced that Gus Simmons has step down from the editorial board and Doug Stinson has been named to take Gus' place. Gilles encouraged electronic submissions. He mentioned an idea for a special issue of the Journal on "Lost Papers of Cryptology". He will explore this idea.

OTHER PUBLICATIONS: Ross Anderson spoke about the publication "Computer and Communications Security Reviews". He has a few copies to pass out during the conference. Ross needs help with reviewing the papers (over 100 papers/month), help in finding more papers to be reviewed and more subscribers to this publication.

CLIPPER/CAPSTONE ISSUE: - Peter remarked that IACR had, through the program for Crypto '93, met its responsibility in educating its members on Clipper. The Board is not planning any future activity in this area.

CONFERENCE PROCEEDINGS: Peter presented the history and results of the Board's discussion on conference proceedings. Around two years ago IACR was notified by Springer that they will no longer provide 200 free copies of the proceedings to the conference. At that time this subject was thoroughly discussed by the Board and an Ad Hoc Committee had been established. At the Board meeting earlier this week the Ad Hoc Committee presented its report and recommendation. The Committee recommended and the Board accepted the following: There will be no pre-proceedings at Crypto and Eurocrypt conferences since the proceedings (Springer LNCS) will be available at the conferences. Springer is the best deal at this time but the Board will continue to monitor. This means that there will be no rump sessions papers in the proceedings; there will be a longer lead time (approximately one month) before the conference for the submission of the papers; and papers will be need to be short (less than 12 pages). This also means that the conference chairman will not need to include the cost of pre-proceedings in the budget and also it will be one less thing to worry about; the Program Chair's job will be easier since after the conference his job is completed; and there will be no delay for obtaining the proceedings.

After Peter's presentation questions were taken from the floor. Peter and others addressed all concerns as best as possible.

GUIDELINES AND PRINCIPLES - Within the Board there are several committees working on preparing and/or revising Guidelines and Principles for General Chairman, Program Chairman, Nomination and Election Committee, and others as deemed necessary by the President and/or the Board.

OPEN ISSUES: There were several topics brought up by the membership at large including parallel sessions, accommodation of exhibits at the conferences, tutorials before or during the conferences, on line papers, etc. All of these issues will be discussed by the Board at Eurocrypt '94. Any member with suggestions or comments to present to the Board should contact Peter or one of the other members of the Board.
Meeting Adjourned.

Conference Reports

CRYPTO'93

event: Crypto'93
date: Aug. 22-26, 1993
where: UCSB as usual
weather: great
general chair: Paul Van Oorschot (Northern Telecom/Bell-Northern Research)
program chair: Doug Stinson (U. Nebraska - Lincoln)
attendee count: higher than recent years (less than peak year of ~265)
total participants: 252
(163 regular, 61 Eurocrypt-attendees, 28 students)
program: excellent as usual (what else would we say?)
38 accepted papers plus 1 invited talk
invited speaker: Miles Smid, NIST
"A status report on the federal government key escrow system"
rump session:
Chaired by Whit; 3 10-minute talks + 12 5-minute talks + panel discussion
10-minute talks
1. Neil Koblitz "Patents: Enemy of Free Scientific Inquiry in Cryptography"
2. Don Coppersmith "Attacking Two Birational Permutation Signature Schemes"
3. Michael Wiener "Efficient DES Key Search"

The highlight (some felt, of not only the rump session but of the whole conference) was a very illuminating panel discussion on Clipper and key escrow. It commenced with the panel members appearing from behind the platform at the front of the room on a rotating platform stage. Many different points of view were expressed in a well-balanced treatment.

panel: Discussion of Key Escrowing
- chaired by Whit
- short talks by: Marty Hellman - How to live with SKIPJACK if you must
Gus Simmons - personal perspective
Amir Herzberg - Trimming the Clipper
Danny Weitzner - Wiretapping and the Law
John Gillmore - information obtain on key escrow via

Freedom of Information Act
as well as Whit, Goldwasser, Rueppel, and Micali

other things different from most Crypto's:
-Cocktail party on Monday eve was held outdoors adjacent to Santa Rosa hall; everyone seemed to like the change (sometimes too hot indoors in past)
-participant photo was taken (not done in quite a few years at Crypto) and distributed (free) to all present
-commemorative souvenir mug with IACR logo - destined to be a collector's item worth millions of dollars in only a few years

best performance/followup of conference:
Andy Clark's presentation during IACR Business Meeting explaining how to not mess-up on the upcoming IACR ballots (e.g. put small envelope inside large envelope, sign name across seal, etc.). Excruciatingly funny because it's impossible for most mortals to mess up the ballot, but even more so given the fact that when the ballots were mailed out, the instructions were on the back side of the ballot which had to be returned, so that after sealing your ballot in the small envelope, you no longer had the instructions on how to complete the enveloping-and-sealing procedure.

Final proceedings: should be very early relative to other years
(pgm chair sent papers in to Springer in November - good work Doug!)

Financial status: will come in under budget, thanks to several factors including larger-than-anticipated attendance.
Final financial details to follow.

PRELIMINARY PROGRAM

Monday, May 9

17.00 - 19.00	Registration and Welcome Cocktail

Tuesday, May 10

08.00 - 09.00	Registration
09.00 - 12.30	Technical sessions
12.30 - 14.00	Lunch
14.00 - 17.30	Technical sessions
19.30	Rump session with buffet

Wednesday, May 11

09.00 - 12.30	Technical sessions
12.30 - 14.00	Lunch
14.00 - 17.30	Technical sessions
18.00	Departure of the tour (Assisi-Foligno)
20.00	Conference Banquet in a typical restaurant in Foligno

Thursday, May 12

09.00 - 12.30	Technical sessions
12.30 - 14.00	Lunch
14.00 - 17.30	Technical sessions
17.30	Closing

****

The program for accompanying persons will be arranged upon request.

PROGRAM COMMITTEE

Ernie Brickell (Sandia Labs., USA)
Claude Crepeau (CNRS, France)
Yvo Desmedt (Univ. of Wisconsin, USA)
Adina Di Porto (FUB, Italy)
Dieter Gollmann (Univ. of London, UK)
Louis Guillou (CCETT, France)
Ueli Maurer (ETH Zurich, Switzerland)
David Naccache (Gemplus, France)
Tatsuaki Okamoto (NTT Labs., Japan)
Jacques Stern (ENS-DMI, France)
Moti Yung (IBM Yorktown, USA)

ORGANIZING COMMITTEE

William Wolfowicz (FUB)
Franco Bertoldi (IIC)
Saverio Cacopardi (Università di Perugia)
Mario Di Fonso (SSGRR)
Michele Elia (Politecnico di Torino)
Giuseppe M. Poscetti (Univ. 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

EUROCRYPT '94

May 9 - 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)

Organized by
Istituto Internazionale delle Comunicazioni (IIC)
Fondazione Ugo Bordoni (FUB)

In cooperation with
Amtec
Italcable
Scuola Superiore G. Reiss Romoli (SSGRR)
Telsy Elettronica Telecomunicazioni
Università di Perugia

VENUE

Conference Room "Aula Magna"
University of Perugia, Italy.

OFFICIAL LANGUAGE

English.

CONFERENCE SECRETARIAT

Istituto Internazionale
delle Comunicazioni - IIC
Via Pertinace, Villa Piaggio
16125 GENOVA GE, Italy
Phone: +39 10 2722383
Fax: +39 10 2722183

GENERAL CHAIRMAN

William Wolfowicz
Fondazione Ugo Bordoni - FUB
Via B. Castiglione, 59
00142 ROMA RM, Italy
Phone: +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
Phone: +39 89 822329
Fax: +39 89 822272
E-mail: ads @ udsab.dia.unisa.it

REGISTRATION

Please fill in the enclosed Registration Form and return it as soon as possible and no later than **April 1, 1994** to the Conference Secretariat.
Forms postmarked after the above mentioned date are subject to pay an extra fee.
Registration Forms sent by fax will be considered as information only.
Registrations will only be accepted upon receipt of payment.

Cancellation

If cancellation is received before **April 1**, a refund of 90% will be made. For cancellations after April 1, there is no refund. Refunds will be dealt with after the conference.

CONFERENCE FEE

The conference fee includes the following:
— Participation in the scientific program.
— One copy of the pre-proceedings.
— Coffee break service and lunch every day.
— Welcome Cocktail on Monday evening.
— Snacks and drinks at the rump session on Tuesday.
— Tour and Conference Banquet on Wednesday.
— Photo of the attendees and souvenir.
— Membership of the IACR for one year.

METHOD OF PAYMENT

The payment — **in Italian Lire only** — must be made by bank cheque payable to:

IIC - Eurocrypt 94.

All banking charges are on the account of the registrants, not of the beneficiary.

HOTEL ACCOMODATION

The official Travel Agent of the Conference is:

Tour Studio Service
Villa Colombella
06080 COLOMBELLA ALTA PERUGIA, Italy
Phone +39 75 691192
Fax +39 75 20857

Room reservations have to be made through the above mentioned Agent. Reservations do not imply any involvement or responsibility of the Conference Organizers. Reservations must be made by returning the enclosed Hotel Booking Form, together with the required deposit and booking charges.

Tour Studio Service has secured a number of rooms, however, it is strongly recommended that reservations are made well in advance. Rooms of the requested rate and category will be assigned as far as possible and on a first come first served basis.
No request will be processed without payment of the corresponding deposit.

Deadline for hotel booking: April 10, 1994.

Cancellation

Tour Studio Service will make no refund for cancellations done after April 26, 1994, since the received deposit will be claimed by the hotels.

CLIMATE

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

TRANSPORT

Perugia can be reached:

from Milano (456 km):
— by plane from Linate Airport (departures at 7.05 and 18.25).

from Roma (170 km):
— by train from Termini Station (departures at 07.30, 10.05, 13.55, 14.50, 15.25, 18.45).
Please note that all the trains stop in Foligno, where it is necessary to take another train to Perugia.
— by bus from Roma Fiumicino Airport (departures at 14.30 and 16.30) and from downtown Roma, Piazza Esedra (departures at 16.00 and 18.00. Arrival: expecting time 2 hrs. later)

Important

A bus service from Roma, Piazza Esedra to Perugia will be arranged on May 9 at 11.00, if a sufficient number of people will request it. **Please tick the appropriate space on the Registration Form.**
Detailed information will be given to the applicants.

EUROCRYPT '94

May 9-12, 1994

University of Perugia, Italy

REGISTRATION FORM

DEADLINE: APRIL 1, 1994

Last Name .... First Name ....

Affiliation ....

Address ....

....

Telephone .... Fax .... E-mail ....

Accompanying person(s) (YES) □ (NO) □

Special dietary requirements? (YES) □ (NO) □ ....

REGISTRATION FEES

— Before April 1, 1994 **(Lit. 430.000)** ....

— After April 1, 1994 **(Lit. 555.000)** ....

— Proceedings (mailed after the Conference) **(Lit. 80.000)** ....

— Tour and Conference Banquet for accompanying person(s) **(Lit 80.000 each)** ....

Total amount Lit. ....

Payment - **in Italian Lire only** - must be made by bank cheque payable to IIC-Eurocrypt 94.
All banking charges are on the account of the registrants, not the beneficiary.

IACR MEMBERSHIP

Payment of the registration fee entitles you to become a member of the IACR.

Do you wish to be an IACR member? (YES) □ (NO) □

This Form and the payment must be addressed to:

ISTITUTO INTERNAZIONALE DELLE COMUNICAZIONI - IIC
Eurocrypt '94 Secretariat
Via Pertinace, Villa Piaggio
16125 GENOVA, Italy
phone: +39 10 2722383, fax: +39 10 2722183

IMPORTANT

I intend to utilize the Bus Service Roma - Perugia arranged by the Conference Organizers on May 9, 1993, departing from downtown Roma (Piazza Esedra) at 11.00 hrs. (fare approx Lit. 15.000) (YES) □ (NO) □

This service will be effected if a minimum number of persons will be reached.

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

EUROCRYPT '94

May 9-12, 1994

University of Perugia, Italy

EUROCRYPT '94 PERUGIA

HOTEL BOOKING FORM

DEADLINE: APRIL 10, 1994

Last Name .... First Name ....

Affiliation ....

Address ....

....

Telephone .... Fax .... E-mail ....

Date of arrival .... Date of departure ....

Accomodation requested (please tick the appropriate space)

Hotel category	Single Room	Double Room
**** super	□ 160.000	□ 236.000
****	□ 95.000/120.000	□ 127.000/144.000
***	□ 97.000	□ 128.000
**	□ 50.000/80.000	□ 70.000/110.000

The rates (in Italian Lire) are per night, including breakfast, taxes and service.

Deposit:	Lit. 100.000
Booking charges:	Lit. 10.000
Total amount due:	Lit. 110.000

PAYMENT MUST BE MADE IN ITALIAN LIRE ONLY.

Please send this Form and a Bank Cheque in the amount due to the order of the official Travel Agent, to the following address:

TOUR STUDIO SERVICE
Villa Colombella
06080 COLOMBELLA ALTA PERUGIA, Italy
phone +39 75 691192, Fax +39 75 20857

As soon as this Form, together with the deposit and the booking charges, will be received, Tour Studio Service will send you the voucher. The deposit (free of bank charges) will be deducted from your final bill.

CRYPTO '94

August 21–25, 1994, Santa Barbara, California

CALL FOR PAPERS

General Information Crypto '94, the Fourteenth Annual **Crypto** Conference, is organized by the International Association for Cryptologic Research (IACR), in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California. Original papers are solicited on all aspects of cryptology.

Topics of Interest The topics of interest include but are not limited too:

- Applications
- Authentication
- Combinatorial Aspects
- Computational Complexity Aspects
- Computer Security Aspects
- Conventional Cryptosystems
- Cryptanalysis
- Cryptographic Hash Functions
- Digital Signatures
- Electronic Money
- Foundations and Theory
- Implementation Aspects
- Information Theoretical Aspects
- Key Distribution
- Number Theoretic Aspects
- Practical Aspects
- Protocols
- Pseudo Randomness
- Public Key
- Secret Sharing
- Standards
- Zero-knowledge

Instructions for Authors Send a cover letter, one title page and 15 copies of an extended abstract to be received by March 4, 1994, (or postmarked by February 23, 1994 and sent via airmail) to the Program Chair at the address given below. The title page should contain the title, the name of the authors, their postal and **e-mail** addresses and the abstract. The extended abstract should start with the title and the abstract, but should be **anonymous**. This should be followed by a succinct statement appropriate for a non-specialist reader specifying the subject addressed, its background, the main achievements, and their significance to cryptology. Technical details directed to the specialist should then follow. A limit of 10 singlespaced pages of 12pt type (not counting the bibliography and clearly marked appendices) is placed on all submissions. Since referees are not required to read the appendices, the paper should be intelligible without them.

Abstracts that have been or will be submitted in parallel to other conferences or workshops that have proceedings are **not** eligible for submission to Crypto. The authors must state compliance to this rule in their cover letter. A LaTeX style file and an example of a cover letter will be available after January 1, by sending e-mail to statuscrypto94@csd4.csd.uwm.edu

Conference Proceedings Crypto '94 will be the first Crypto conference where **proceedings will be available at the meeting**. These proceedings will be published in the Springer Verlag's Lecture Notes in Computer Science. Clear instructions about the final copy will be sent to authors of accepted papers. The final copies of the accepted papers will be due on June 8, 1994. Final papers arriving too late will be *removed from the main program*. Authors of accepted papers must guarantee that their paper will be presented at the conference.

A limited number of stipends are available to those unable to obtain funding to attend the conference. Students whose papers are accepted and who will present the paper themselves are encouraged to apply if such assistance is needed. Requests for stipends should be addresses to the general chair.

Program Committee

Yvo Desmedt, Chair, University of Wisconsin – Milwaukee, USA
Tom Berson, Anagram Laboratories, USA
Don Coppersmith, IBM T. J. Watson Research Center, USA
Donald Davies, United Kingdom
Shimon Even, Technion, Israel
Amos Fiat, Tel Aviv University, Israel
Russell Impagliazzo, University of California San Diego, USA
Ingemar Ingemarsson, University of Linkoping, Sweden
Mitsuru Matsui, Mitsubishi Electric Corporation, Japan
Alfred Menezes, Auburn University, USA
Andrew Odlyzko, AT&T Bell Laboratories, USA
Jennifer Seberry, University of Wollongong, Australia
Ben Smeets, Lund University, Sweden
Moti Yung, IBM T. J. Watson Research Center, USA

Important Information

Submission receipt deadline: March 4
(or postmarked airmail: February 23)
Notification sent to authors: April 25
Final copies due: June 8, 1994

Send submissions to:

Yvo Desmedt, Program Chair Crypto '94
Dept. of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario
Canada, N2L 3G1
Internet: desmedt@cs.uwm.edu
Fax: before January 26: +972 (4) 294353
after January 26: +1 (519) 746-3077

For other information, contact:

Jimmy R. Upton, General Chair
Uptronics Incorporated
1590 Oakland Road
Suite B203
San Jose, CA 95131
USA
Internet: jupton@netcom.com
fax: +1 (408) 451-8901

ASIACRYPT'94 - Call for Papers
University of Wollongong, NSW, Australia
November 28 - December 1, 1994

The Asiacrypt'94 conference is a continuation of the Auscrypt'90, Asiacrypt'91 and Auscrypt'92 conference series.

The Asiacrypt conferences are the third, after Crypto and Eurocrypt, and the youngest stream of workshops devoted to the theory and applications of cryptology.

Asiacrypt'94 is sponsored by the University of Wollongong, Australia, in cooperation with the International Association for Cryptologic Research. The conference will be held on the University of Wollongong campus, Wollongong, New South Wales, Australia.

Instructions for authors:
Authors are invited to submit original papers, neither published nor submitted for publication elsewhere, by sending 14 copies of an extended abstract containing at most 10 pages of 12pt type (title page and bibliography are not counted) to the Program Chair.

Extended abstracts should begin with a succinct statement of the problem, the results achieved, their significance, and a comparison with previous work. They should be written in a manner understandable to a non-specialist reader. Technical exposition directed to the specialist should follow as needed.

Submissions must be anonymous - names and affiliations of the authors should be displayed on the title page of only one copy, which will be used by the Program Chair to keep track of the submissions. The other 13 copies should give the title of the paper with no indication of who the authors are.

Important dates:
- DEADLINE for submissions July 18, 1994 (submissions received after July 25, 1994 will be rejected),
- ACCEPTANCE or rejection of submissions September 26, 1994,
- FINAL versions of extended ABSTRACTS (no more than 10 pages) October 17, 1994,
- FINAL versions of PAPERS for conference proceedings January 8, 1995 (the proceedings are expected to be published in Springer-Verlag's Lecture Notes in Computer Science).

Program Committee:
J. Pieprzyk (Chair, University of Wollongong, Australia),
D. Beaver (Pennsylvania State University, USA),
E. Biham (Technion, Israel),
C. Chang (Chung Cheng University, Taiwan),
Z. Dai (Academia Sinica, PROC),
Y. Desmedt (University of Wisconsin, USA),
T. Itoh (Tokyo Institute of Technology, Japan),
T. Matsumoto (Yokohama National University, Japan),
A. Odlyzko (AT&T Bell Laboratories, USA),
T. Okamoto (NTT, Japan),
B. Preneel (Katholieke Universiteit Leuven, Belgium),
R. Rueppel (R^3, Switzerland),
R. Safavi-Naini (University of Wollongong, Australia),
Y. Zheng (University of Wollongong, Australia).

Program Chair:
Josef Pieprzyk
Department of Computer Science
University of Wollongong
NSW 2522, Australia
Phone: +61 42 213872
Fax: +61 42 214329
e-mail: josef@cs.uow.edu.au

General Chair:
Jennifer Seberry
Department of Computer Science
University of Wollongong
NSW 2522, Australia
Phone: +61 42 214327
Fax: +61 42 214329
e-mail: jennie@cs.uow.edu.au

WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC '94)
May 5 & 6, 1994

Location:

Walter Light Hall
Department of Electrical Engineering
Queen's University
Kingston, Ontario K7L 3N6

Invited Speakers:

Michael Wiener, BNR: "Efficient DES Key Search", Thursday a.m.
Richard Kemmerer, UCSB: "Three Systems for Cryptographic Protocol Analysis", Friday a.m.

Organizers:

Carlisle Adams, BNR
Henk Meijer, Queen's
Stafford Tavares, Queen's
Paul Van Oorschot, BNR & Carleton University

Registration:

Regular, $150.
Student, $ 40.

Registration includes a copy of the proceedings, social event, lunches and coffee breaks.

Themes:

- *Design and analysis of Secure Private-key Block Ciphers*
- *Formal Methods for Cryptographic Protocols*
- *Related Topics*

General:

The workshop will start at 10:30 a.m. on Thursday, 05 May. On Friday, we begin at 9:00 a.m. and end at 4:30 p.m. There will be a social event on Thursday evening. The program will be single stream and each presentation slot will be 30 minutes. Active discussion and participation are encouraged.

Invitation:

Researchers interested in the theme topics are invited to submit 4 copies of a six page summary for consideration by 01 February, 1994. Notification of acceptance will be given by 04 March, 1994. Accepted papers will appear in a proceedings (12 page limit). Camera-ready copy for the proceedings is due 04 April, 1994. Submit summaries to Stafford Tavares at the address given above.

Phone:	*613 545-2945 or -2925*
FAX:	*613 545-6615*
email:	*tavares@ee.queensu.ca*

WORKSHOP ON SELECTED AREAS IN CRYPTOGRAPHY (SAC '94)
May 5 & 6, 1994

REGISTRATION FORM

(PLEASE TYPE OR PRINT)

Name: ______________________________ Student? □Yes □ No
Last First

Mailing Address: ____

____
City Province/State Postal Code/Zip Code Country

Phone: ______________ FAX: ______________ Email: ________________

REGISTRATION FEE (Payable before April 15, 1994) :
Regular Registration: $150. $ __________
Fulltime Graduate Student: $ 40. $ __________

(Registration Fee includes a copy of Proceedings, dinner on Thursday evening, lunches and coffee breaks.)

ACCOMMODATION:
Victoria Hall, Queen's University: $43. per day per person (includes room, breakfast, parking and tax). **Please note that Victoria Hall is not available on Wednesday night.** Telephone: 613-545-2531, FAX: 613-545-6759.

□ Single □ Double Sharing Room with: ________________________

Thursday night: $__________ @ $43.00 per person $ __________
Friday night: $ __________ @ $43.00 per person $ __________
Please make cheque payable to "Queen's University". Total Amount Enclosed $ __________

Attractive bed & breakfast is available at the Hochelaga Inn and the Rosemount Inn. Some nearby hotels are the Holiday Inn, Ramada Inn and Howard Johnson. The telephone and fax numbers and addresses are:

	Single Rates Start At:	Telephone No.	Fax Number
Hochelaga Inn, 24 Sydenham St.	$ 73.	613-549-5534	613-549-5534
Rosemount Inn, 46 Sydenham St.	$ 65.	613-531-8844	613-531-9722
Holiday Inn, 1 Princess St	$ 95.	613-549-8400	613-549-3508
Ramada Inn, 1 Johnson St.	$ 85.	613-549-8100	613-547-3241
Howard Johnson, 237 Ontario St.	$ 99.	613-549-6300	613-549-1508

Abstracts from Recent Theses

Title: Principles for the Design of Hashing Algorithms

Author: Babak Sadeghiyan

Supervisors: A/Prof. Josef Pieprzyk, Dr. Lawrie Brown

Institution: University College, ADFA, University of New South Wales,

Abstract:

There have been many proposals for secure hash algorithms, and some of them have been in use for a while. However, many of them have proved insecure. One of the major reasons for this is the progress in technology. The failed effort of many researchers suggests that we should work on some guidelines or principles for the design of hash functions.

The thesis presents principles for the design of secure hash algorithms. Hash algorithms are classified based on whether they apply a block cipher as the underlying one-way function or not.

It is shown that for a block-cipher-based hash scheme, if the underlying block cipher is secure against chosen plaintext/ciphertext attack, the hash scheme is secure against meet-in-the-middle attack. Based on DES-like permutations and assuming the existence of pseudorandom function generators, new structures for hashing algorithms are studied.

Non-block-cipher-based hash functions include a spectrum of many different proposals based on one-way functions from different branches of mathematics. These hashing systems are generalized and a new construction of hash functions are developed, assuming the existence of a one-way permutation. The generalized constructions are improvements upon the Zheng, Matsumoto and Imai's hashing scheme, based on the duality between pseudorandom bit generators and hash functions, but they incorporate strong one-way permutations. It is shown that we can build such strong permutations with a three-layer construction.

Two schemes for the construction of families of strong one-way permutations are also proposed.

The following letter was submitted to the National Institute for Science and Technology by one of our members. The opinions expressed are those of the author and do not necessarily reflect those of the editor or the IACR.

UNIVERSITY OF WISCONSIN MILWAUKEE

College of Engineering and Applied Science
Department of Electrical Engineering and Computer Science

UWM

September 24, 1993

Director, Computer Systems Laboratory
ATTN: Proposed FIPS for Escrowed Encryption Standard
Technology Building, Room B-154
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Mr. Director:

I want to take this opportunity to express my concerns about and opposition to the "key escrow" proposal that enables the government to eavesdrop on the communications of Americans with the Clipper encryption technology.

The proposed bugging of data and voice communications of the nation is being presented as a necessary measure to supposedly protect "law enforcement" and "national security" interests.

What is being proposed threatens one of the most fundamental constitutional rights: the right to privacy. There is a tendency to view cryptography as a weapon, the official view of the intelligence agencies. That is no more true for cryptography than for ordinary locks and keys, since, after all, cryptography pertains to the design of locks and keys for data protection. The fact of the matter is that many of our assets are no longer physical, but *logical*. If we allow the constitutional protection against search and seizure to lapse just because technology has changed the nature of certain things would mean that we have to throw away a great many parts of the constitution because new technologies can change other concepts of where one's possessions and even physical self begin and end.

There is widespread agreement that criminals, especially smart ones, will not use a bugged device to conduct their business. It is important to consider the options of the criminal. Does the criminal have to use the bugged system? The answer is certainly no. Criminals, especially the ones that are being touted as the targets of the system, drug dealers and terrorists, are well funded. They will have no problem getting computer hackers to build them hardware and software systems to implement their own cryptographic systems. Computer specialists are hardly more immune to the lure of money or intimidation than other professionals. Moreover, if cryptography is essentially outlawed, as is being contemplated in FOIA obtained internal memoranda of the government, then the only people with access to quality cryptographic systems and services will be criminals. To paraphrase that old battle cry, "If you outlaw cryptography, only outlaws will have cryptography". Not only can criminals encrypt their messages, they can also hide the ciphertext with techniques of information theory to make it look innocuous. Already the effects of government control is taking its toll on research in cryptography: the number of papers on design of new systems is miniscule compared to the number of papers that deal with the one or two systems in place. In addition, the availability of hardware and software, that is sorely needed for the protection of computer systems and data, is so limited given our incredible technological advances that from a protection point of view we are in fact a "cryptographic third world".

In view of the fact that criminals will have access to the technology that is being denied law abiding citizens, one must ask then: just what targets will be left to evesdrop on? Ordinary Americans, politicians, dissidents, labor leaders, ... to name a few. This proposal, when considered with its monster twin, the proposed digital signature standard, DSS, a sort of government approved no-other-pens-allowed BIC pen, amounts to a national dragnet.

Some supporters of this major violation of privacy say that it is no worse than, say, arrest. It is absolutely worse than arrest. It is done secretly. It attempts to predict that a person is about to commit a crime. If the right to privacy can be violated on suspicion that a crime might be committed, other rights will be violated too. It is difficult to see how one can draw the line at just privacy, one of the most sacred rights in this country. There is no doubt as to what is next: preventive detention; observe how people walk, talk and think to themselves and put them away, well before they have done anything.

The consequences of privacy violations is not all that apparent to some members of the crypto community. Some may be unaware of the bugging, ridicule and assault of even prominent members of the various minorities. One hardly needs to mention the bugging of Martin Luther King, harassed by the FBI. But some might say that was in the past. Well one does not have to go back that far in time. More recent events involving a Governor of a State show that this type of intimidation is continuing. As the country's multicultural pot becomes ever more mixed, we hardly need to put in place tools for abuse of one race or religion by another that may be momentarily in control of the devices.

Still other Americans have been the subject of bugging, allegedly by foreign governments. Consider the case of Andrew Young, the US ambassador to the United Nations. He was forced to resign, allegedly because his conversations were bugged by Israel. If someone of the rank of ambassador can be brought down, it is difficult to imagine how anyone can be safe. Other governments will no doubt have a stake in getting rid of government officials who don't suit them. Dissidents from other countries who take refuge here will hardly be safe with such a wholesale bugging system. After all intelligence agencies cooperate with even the most human rights abusive governments. Such governments will no doubt need "favors" from time to time.

It is interesting to note that at the CRYPTO-93 meeting, fear was expressed that the "Biden" bill might become reality. This was in reference to an attempt by Senator Joseph Biden to put severe restrictions on the use of cryptography. Senator Biden is chairman of the Senate Judiciary Committee, which blocked the nomination of Judge Robert Bork to the Supreme Court because of concern about *privacy*. This is certainly a change in perception of just who is a threat to privacy.

Finally, even the very name of this proposal for systematic bugging, "escrow", is deceptive. Consider the very definition of "escrow" (Webster's dictionary):

- a deed, a bond, money, or piece of property held in trust ...

Privacy held in trust? By Police? By Intelligence agents and their friends? It is impossible to imagine how one's privacy can be taken back after it is violated. Holding privacy in escrow is like holding someone's wife in escrow for a night. This is no escrow. This is an indecent proposal.

Sincerely

George I. Davida
Professor

cc: