

IACR

NEWSLETTER

**A Publication of the International Association
for Cryptologic Research**

Volume 9 Number 2 June 1992

CONTENTS

Editor's Corner	1
(The New) President's Message	2
Minutes of BoD meeting	3
Conference Reports (Past, Present and Future)	
Report on EUROCRYPT '92 - Balatonfüred, Hungary	12
CRYPTO'92 - Santa Barbara, USA	15
AUSCRYPT 92 - Gold Coast, Australia	23
EUROCRYPT'93 - Lofthus, Norway	27
Announcement - Special Issue of JoC	28
Notice Board (etc., etc., etc.)	29

IACR Contact List

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

Officers . . .

President

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

Vice President

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

Secretary

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

Treasurer

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

Eurocrypt 92 Chair

Tibor Nemetz
Math. Inst. of the Hungarian
Acad. of Sci.
P.O. Box 127/11-1364
Budapest, Hungary
h1137nem@ella.hu

Crypto 92 Chair

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

Newsletter Editor

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

J. Of Cryptology Editor

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

Directors . . .

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

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

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

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

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

John Gordon
Lynfield House
Datchworth Green, Herts. SG3 6TL
United Kingdom
+44 438 811015

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

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

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

Editor's Corner

I see by my calendar that June has rolled around again, so it must be time for another issue of the newsletter. Many things have happened since the last issue: the new officers and directors of the IACR have assumed their posts, 233 of us went to Hungary and the program for CRYPTO'92 has just been released.

As most of you are aware, we have a new President, Secretary and three directors (Ingemar Ingemarsson and Kevin McCurly are continuing as Vice-President and Treasurer respectively). Tom Berson has stepped down after four years at the helm of the IACR. As the new President mentions in his report, the current strength and vitality of the IACR is due in a large part to Tom's work. I would like to add my own thanks to Tom for his help and support (and we cannot forget Dorothy Berson's contributions to the IACR - Thanks Dorothy!). The good news is that Tom was elected as a director of the IACR.

Many thanks are also due to Rainer Rueppel who held the post of Secretary until last fall.

I would like to welcome Peter Landrock as the new President of the IACR. Peter has been involved with the IACR for many years and I'm sure that the IACR will be well served by his leadership.

I'd also like to welcome our new Secretary, Sherry McMahan who has also contributed to the IACR over many years (General Chair CRYPTO'90). I'm sure she will do an outstanding job!

Two new faces join the ranks of our directors: Andrew Clark (our host at EUROCRYPT'91) and Hideki Imai (Program Co-Chair for Asiacrypt'91) - as mentioned before, Tom Berson was also elected as a director). To the outgoing directors - Thomas Beth, Ernie Brickell and Norbert Cot, many thanks for all of your contributions.

An important item that requires the attention of the membership is the upcoming election for directors. The terms of David Chaum, Whit Diffie and John Gordon expire at the end of this year. A nomination committee has been set up consisting of Andy Clark, Yvo Desmedt and me (Gord Agnew). The important dates to remember are :

Nominations close September 15, 1992

Ballots will be mailed not later than October 1, 1992

Ballots must be received by November 15, 1992

Other news includes the resounding success of EUROCRYPT'92 in Hungary. Tibor Nemetz was our host and deserves our thanks for putting on a great conference. Rainer Rueppel is also to be congratulated for putting together an excellent program.

I'm running out of space, so I will finish by saying I look forward to seeing everyone at CRYPTO. GBA.

(Notes from the EUROCRYPT Dinner: AC UTN DTTC)

President's Message

Dear Members,

It has been an exciting year for cryptography. Applications are really moving forward. The first international standard in cryptography (ISO 9796) is finally in place, seconded by the NIST draft DSA. Zero-knowledge seems to become public knowledge, and a proposal for integration of security services in EDIFACT has been worked out by the Security Joint Working Group formed by the UN/EDIFACT Board.

This brings a lot of attention to cryptologic research, which leaves IACR and its members with even greater responsibility.

Within the Society, the past year has been both dramatic and exiting:

Crypto'91 was excellently handled by Burt Kaliski Jr. as General Chair, with perhaps the greatest surprise ever at Crypto conference: The beach barbecue was canceled - due to rain! Instead, the dining hall was quickly transformed into an adequate setting for an elegant dinner with classical music. Thanks to Burt, as well as the Program Chair, Joan Feigenbaum, for running everything so smoothly and efficient. The importance of all the efforts our members are putting into these responsibilities cannot be overestimated. The IACR exists because of its conferences, and CRYPTO at U.C. Santa Barbara has become a corner stone in our activities.

Asiacrypt'91 was the first Asiacrypt conference ever and thus a historical event. This was done in cooperation with IACR, which is of less formal connection to IACR than Eurocrypt and Crypto. Kenji Koyama served as General Chair, while Hideki Imai and Ron Rivest co-chaired the Program, and they all did a great job. The conference took place at the foot of beautiful Mt. Fuji, and was a great success in every respect, which set a great model for future Asiacypts. The Japanese barbecue was an absolute delight.

Eurocrypt'92 was yet another historical event in that it took place in a country which now once again belongs to Central Europe. The General Chair, Tibor Nemetz had put the utmost care into the preparation, which included a great number of social events, thus providing welcomed distractions to the program, Rainer Rueppel had put together. A completely new ingredient was a panel discussion on key generation, inspired by the sometimes quite heated discussions on RSA versus DSA. The discussion was very fair and constructive, due to excellent conduct by Rainer. We congratulate both with a successful conference.

Another event, which hopefully will not be too noticeable, is that Tom Berson has stepped down after four successful years as president of the IACR, preceded by his serving as chancellor. I know Tom has been extremely popular, and with very good reason. He is very inspiring to work with, and I am very glad to have him as a director and pillar in my private backing group. During his reign, IACR has come of age, with more than 800 members, and an excellent journal. I am confident all members will join in a great Cheer for Tom!!

Journal of Cryptology now has a new editor-in-chief, Gilles Brassard, who cannot even be hindered in his task by a nasty Canadian post-strike! As per volume 6, we will see 4 annual issues rather than 3, reflecting the fact that the Journal is extremely well and alive. Tom, after having step down as president, has negotiated a very satisfactory contract with Springer.

Incidentally, Springer has been contacted by Robert Redford's office in Hollywood (honestly!), requesting permission to use JCrypt in a new thriller, Sneakers, now in production. Apparently, Redford plays a spy trying to solve a cipher. He is at his desk, working, deeply engaged in JCrypt, which - Springer has promised - will be "displayed prominently". The society has given its consent, and will now try to negotiate a minor part in the picture for the new president! I expect Bob to call back any minute now.

One more issue: We are now very close to a new logo, which will be presented at Crypto'92, which has the great advantage that it will be available in postscript.

This was all history! But Crypto'92 is coming up very soon, and I look very much forward to seeing all of you either there or at Auscrypt'92, the second Auscrypt in history, in December.

Peter Landrock

MINUTES FROM IACR BOARD OF DIRECTORS MEETING
MAY 1992

The IACR Board of Directors meeting was held on 25 May, 1992 in Balatonfured, Hungary at the Eurocrypt '92 conference. The meeting was called to order by the president, Peter Landrock. In attendance were Jennifer Seberry, Yvo Desmedt, Tom Berson, Andy Clark, Kevin McCurley, Gordon Agnew, Tibor Nemetz and Kenji Koyama (with Hideki Imai's proxy), Neil Ferguson (with David Chaum's proxy), Ernie Brickell (with Gilles Brassard's proxy), Whit Diffie, Sherry McMahan and Peter Landrock (also with Ingemar Ingemarson's proxy).

The Agenda was approved with several additions under new business and with some of the Crypto conferences reports presented first.

Crypto '93: Nominations for the general chair were discussed. The final decision for general chair and program chair will be finalized at Crypto '92.

Crypto '92: General chair is Spyros Magliveras and Program Chair is Ernie Brickell. Conference is to be held in Santa Barbara from 16 to 20 August, 1992. Ernie reported that there were 136 papers received and at most 44 will be accepted. Talks for the rump session will be chosen from papers that fall into three categories: 1) humorous paper; 2) controversial subject; and 3) a talk that has good results and would have been accepted as a regular paper if submitted in time. There will also be a poster session. Instructions will be included in the IACR Newsletter. In the Newsletter there will be made a correction to the registration form in reference to Eurocrypt '92 versus Eurocrypt '91.

The other conference reports will be given later.

- 1) Peter Landrock welcomed everyone and spoke about the transition from Tom Berson's presidency. He postponed to express the gratitude of IACR to Tom until the General Assembly Meeting on Wednesday.
- 2) The minutes from the last Board of Directors meeting at Crypto '91 have been approved and distributed in the January IACR Newsletter.

The minutes from this meeting will be distributed to each of the directors for comments/corrections and be published in the next IACR Newsletter.

- 3) Jennifer Seberry reported on the election results. There were 400 votes and although there was an increase in the IACR membership at AsiaCrypt '91 there were not many write in votes.

Thanks to Jennifer, David Chaum and Gord Agnew for their efforts in this election.

The issue of new members and when they are eligible to vote was discussed. There should be a point of clarification for the ByLaws. (Sherry to make a note.)

- 4) Report on Crypto '91: In IACR newsletter-227 in attendance. Proceedings have been mailed.
- 5) Report on AsiaCrypt '91: Kenji Koyama gave the report (see attached). He encouraged future conferences in Asia (Asiacrypt's) to be held.
- 6) Financial Report by Kevin McCurley: (see attached). The monies will be divided into two accounts because of the limited insurance coverage of \$100,000. The 1991 Tax Return is available for anyone who wishes to have a copy. Contact Kevin for a copy.

Thanks to Kevin for a great job.

- 7) Ernie Brickell spoke on behalf of Gilles Brassard concerning the Journal of Cryptology. Gilles has recommended that the Journal be increased to four issues per year. Two issues of 64 pages and two of 48 pages in 1993. Discussion on this followed later.

Tom Berson gave a report on the negotiations with Springer. By the direction of the Board of Directors, Tom spoke with Springer concerning the renewal of the contract which will end December '92. Tom has with him copies of the contract for Peter's signatures. The cost per copy of the journal has been increased and with the recommendations from Gilles the journal will be increased to four issues per year. The Board members and editorial committee members will receive advance copies of the Journal. Labels for the mailings will be sent by IACR to Springer. The new logo will be incorporated (see discussion on logo); there will be an increase in the quality of the reprints, more promotion will be done by Springer and fifty free reprints will be available to each author.

Tom and Ernie both support Gilles recommendation to increase the number of issues of the Journal from three to four.

- 8) Discussion of membership fees: There are approximately 820 members at this time (this is the number of the latest mailing of the Journal and will fluctuate with each conference where the majority of members join each year.) Since the increase of the cost of the Journal and the proposed increase of number of issues per year, it will be necessary to increase the membership dues of IACR. The discussion was on how much the increase should be. This must be presented to the general membership at the Official Assembly at Crypto '92 in August.

** Further discussions on the proposal from Springer concerning the proceedings. Springer has agreed to ship 75 copies bulk to one author. Anything over 75 copies will be sold to IACR at 33% of the regular sales price. Springer usually sells an additional 500 copies to libraries, etc. Discussion deferred to later.

- 9) Eurocrypt '94 proposal:

William Wolfowicz of Italy proposed that Eurocrypt '94 to be held in Perugia, in the heart of Italy. There is a population of 300,000 with 30,000 students. There is an university there for foreigners which means that there is some English spoken in the area. The University has agreed that the conference room will be available at no charge. There are rooms available at the monastery and also there are hotels within five minute walk. Meals can be held inside or out. There are two flights per day from Milan and there are trains and rental cars from Rome. There will also be bus transportation provided for the conference from the Rome airport.

The proposal was accepted with the following vote: for - 11, against - 0, abstain - 1.

It was proposed that William Wolfowicz be the general chairman and Alfredo de Santis be the program chairman. The votes was: for - 10, against - 0; abstain - 2.

Report on Eurocrypt '93:

Kare Presttun gave a report of the progress on the planning for Eurocrypt '93. The conference is to be held from 24 to 27 May, 1993 at Hotel Ullensvang, Lofthus, Norway.

** Discussion on Journal:

Tom Berson moved that the number of issues per volume be increased according to Gilles' plan. Andy Clark seconded the motion. This passed with the following vote: for - 8; against - 2; abstain - 2.

** Membership dues:

Motion by Kevin McCurley to propose an increase of the fees to \$50 and this was seconded by Gord Agnew. Passed with the following vote: for - 12; against - 0; abstain-0.

Kevin to present to the General Assembly at Crypto '92.

** Conference pre-proceedings/proceedings discussion:

There was a motion and it was accepted to consider having the proceedings replace the pre-proceedings. This will require that high quality camera ready copies of the papers be provided at the conferences and the same papers published as the official proceedings. Tom and Andy are to discuss with Springer. Kevin will also talk with IEEE concerning publishing the proceedings. This will be discussed at Board of Directors meeting at Crypto '92.

- 10) Auscrypt '92: To be held on the Gold Coast in Queensland, Australia from 13 to 16 December. General Chair: Bill Caelli and Program Chair: Jennifer Seberry. Call for papers by 11 September to be sent to Jennifer Seberry.

11) LOGO:

At the request of the Board of Directors, David Chaum had taken the proposed logos and had them refined. These were presented by Peter. One of the designs were chosen with the following vote: for - 8; against - 1; abstain-2.

There will be a hash function computed. Peter to contact David for a postscript copy for Newsletter, etc. A hard copy will be sent to Springer.

12) Future Strategy:

There was a short discussion about whether national chapters are desirable. Further discussion at the next meeting of the board.

13) Mailing List:

The mailing list will be updated as necessary. All effort is being made to keep an accurate mailing list. The list will be maintained by Peter Landrock.

14) Nominating Committee for 92 Elections:

Accepted for the committee were Andy Clark, Gord Agnew and Yvo Desmedt.

15) ICSU Affiliation:

Discussion deferred to the next meeting.

16) Memorials:

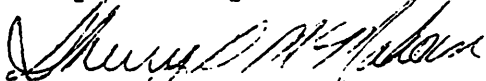
Newsletter will carry memorials.

17) Old Business:

Tom has heard from John McHugh that the IEEE Security and Privacy Committee is content to stay within IEEE and no further action is required from IACR.

18) Meeting adjourned.

Respectfully submitted,



Sherry S. McMahan
Secretary
29 June, 1992

Attachments:

AsiaCrypt '91 report
Financial Report and Balance Sheet (2 pages)

MINUTES
IACR General Assembly
Eurocrypt '92, Balatonfured, Hungary
Wednesday, 27 May, 1992

The IACR general assembly was called to order by the president, Peter Landrock.

1. Peter gave a special thank you and a letter of appreciation to Tom Berson for his contribution as president of IACR.
2. Nominating committee for the 1992 elections was introduced.
3. Peter introduced the officers and directors of the IACR.
4. Peter gave thanks along with letters of appreciation to Tibor Nemetz, General Chair of Eurocrypt '92 and Rainer Rueppel, Program Chair of Eurocrypt '92.
5. Peter gave an update on the Journal of Cryptology and the Newsletter.
6. Conferences: Crypto '92, 16 - 20 August, 1992 in Santa Barbara; Auscrypt '92, 13 - 16 December, 1992 on the Gold Coast, Queensland, Australia; and Eurocrypt '93, 24 - 27 May, 1993, Lofthus, Norway. Crypto '93 will be held from 22 to 26 August in Santa Barbara. Eurocrypt '94 will be held in mid-May, 1994 in Perugia, Italy.
7. The new address for the IACR is: IACR, Inc., The Science Park Gustav Wieds Vej 10, 8000 Arhus C, DENMARK
email: IACR@daimi.aau.dk
8. Peter presented the new IACR logo.
9. Kevin McCurley gave the financial report and stated that the 1991 tax return is available to anyone who would like a copy.
10. Open Discussion: The subject of moving Crypto from Santa Barbara- this would most likely result in an increase in fees along with complicating the preparation. For now the Crypto conference will continue to be held in Santa Barbara.

Ed Dawson mentioned a few words on Auscrypt '92.

Meeting adjourned.

Sherry S. McMahan
29 June, 1992

Report on ASIACRYPT'91

May 26, 1992

Kenji Koyama, NTT, Japan

- It was held from November 11 to 14 at the Hotel Highland Resort, Fuji-yoshida, Japan
- Number of participants: 188 (121 from Japan, 67 from 16 foreign countries)
- Number of new IACR members: 139
- Technical Session: 40 talks, 4 invited talk, (12 talks in Rump Session)
- Security Products Show: 9 companies
- Proceedings will be published in Lecture Notes in Computer Science from Springer.

We appreciate for sponsorship and kind support of IACR and the members.

IACR FINANCIAL ANALYSIS FY 1991

EC 91 (*) Crypto 91 YEAR TOTAL

-----CONFERENCE INCOME-----

311	seed money	2000.00	2000.00	
321	registration fees	84615.71	40400.00	125015.71
322	room and board	30963.68	44950.00	75913.68
331	grants	5359.67	0.00	5359.67
391	interest	3464.43	811.74	4276.17
399	other	12327.57	2758.10	15085.67
TOTAL INCOME		138731.06	90919.84	229650.90
(-membership)		11040.00	6800.00	17840.00
TOTAL INCOME		127691.06	84119.84	211810.90

-----CONFERENCE EXPENSE-----

411	seed money return	2000.00	2000.00	
422	room and board	30539.19	43367.79	73906.98
431	Publicity	1468.82	1915.37	3384.19
432	Org/lcl arrngmnts	12091.71	5976.35	18068.06
433	meeting facility	26494.47	3444.50	29938.97
434	reception/banquet	20617.17	18293.74	38910.91
441	invited lecturers	0.00	600.00	600.00
442	travel assistance	0.00	1399.12	1399.12
451	proceedings	6735.31	5428.57	12163.88
499	other	591.26	157.63	748.89
TOTAL EXPENSE		100537.92	82583.07	183120.99

SURPLUS

481	PAID TO IACR			
	membership	11040.00	6800.00	17840.00
	surplus	27153.13	1536.77	28689.90
	ASIACRYPT 91			5560.00
TOTAL		38193.13	8336.77	52089.90

* Figures for EC 91 are approximate dollar figures

ATTENDEES

(EC attendees)		56
regular	248	138
student	28	32
total	276	226

BALANCE SHEET

ASSETS

	31Dec90	31Dec91	
Checking	62346.44	73778.94	
Savings		30781.21	
receivable C 92		2000.00	
EC 90 memb	10100.00		
EC 90 surplus	82.88		
EC 90 seed	2000.00		
C 90 memb	5800.00		
C 90 surplus	881.18		
C 90 seed	2000.00		
C 91 memb		6800.00	
C 91 seed	2000.00	2000.00	
C 91 surplus		1536.77	10336.77
1 registration		-160.00	
TOTAL ASSETS	85210.50	116736.92	

LIABILITIES

EC 89 Proceedings	4493.50		
EC 90 Proceedings	285.00		
J of C Volume 3	13000.00		
C 90 Proceedings	1567.91		
C 91 proceedings		1069.16	
J of C Volume 4		12025.00	
TOTAL LIABILITIES	19346.41	13094.16	

FY91 SUMMARY OF NON-CONFERENCE EXPENSES

Printing	44.65
Supplies	34.59
Legal & Prof.	150.00
EC89 Proc.	4493.50
EC90 Proc.	285.00
EC91 Proc.	2921.59
C 90 Proc.	1572.91
J. of C.	13000.00
Newsletter	2485.84
Bank Charges	91.80
Postage	662.55

General Chair's Report

EUROCRYPT '92

May 24--28, 1992 Balatonfüred, Hungary

The conference was sponsored by the International Association for Cryptologic Research (IACR), and was organized in association with the Mathematical Institute of the Hungarian Acad. of Sci.. The conference site, Balatonfüred is located at the northern shore of the largest lake in Central Europe: Lake Balaton.

The conference was attended by 233 participants (including 27 students) from 29 countries, and accompanying persons. The increase in the number of local attendees (last year 5, now 15) did not compensate the decrease of the number of last years home attendees (Great Britain, last year 55, now 14).

The geographical representation was as follow:

Australia	3	Austria	11
Belgium	4	Canada	3
China (People R.)	3	Czechoslovakia	1
Denmark	7	Egypt	1
Finland	1	France	26
German	38	Great Britain	14
Hungary	15	Ireland	1
Israel	2	Italy	12
Japan	6	Netherlands	10
Norway	3	Romania	3
Saudi Arabia	1	Singapore	2
South Africa	5	South Korea	3
Spain	4	Sweden	14
Switzerland	10	USA	28
Yugoslavia	2		

On the arrival day evening an informal meeting took place with wine and snacks. Monday evening we had a welcome dinner at a Restaurant in Szentbékállá, 30 km scenic drive away from the conference site. The conference banquet was held in the Hotel's restaurant on Wednesday (27th May).

The highlight of the conference of course was the material presented, and congratulations must go to the Programme Committee:

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

Their work was excellently coordinated by the Programme Chairman:

Rainer A. Rueppel
(R^3 Security Engineering,
Bahnhofstrasse 242, CH--8623 Wetzikon, Switzerland).

There were 80 submissions for presentation. Based on their extended abstracts of 8--12 pages, the International Program Committee invited 34 of them. They were clustered around 12 sessions.

SESSION 1 : SECRET SHARING

SESSION 2 : HASH FUNCTIONS

SESSION 3 : BLOCK CIPHERS

SESSION 4 : STREAM CIPHERS

SESSION 5,7 : PUBLIC KEY I., II.

SESSION 6 : FACTORING

SESSION 8 : PSEUDO -- RANDOM PERMUTATION GENERATORS

SESSION 9,12 : COMPLEXITY THEORY AND CRYPTOGRAPHY I., II.

SESSION 10 : ZERO -- KNOWLEDGE

SESSION 11 : DIGITAL SIGNATURE AND ELECTRONIC CASH

All accepted abstracts were printed in a volume of Extended Abstracts and distributed among the participants. 14 left-over copies had been sold. The final Proceedings of the conference is planned to be published in the Springer' Lecture Notes in Computer Sciences.

This year László Csirmaz organized the Rump session. It was relatively short, in less then 3 hours 12 papers of 10 minutes were presented. (Submitted papers were screened, and some of them were rejected.)

Besides the contributed talks, a Panel Discussion on DSS was organized under the title *Trapdoor Primes and Moduli*.

I would like to record my personal thanks to members of the Hungarian Organizing Committee who made my work easier: László Csirmaz (Math. Inst. of the Academy), Gyula Katona (Eötvös Univ.), Ferenc Ledniczky (retired from Defence), István Vajda (Technical Univ).

The assistance of Malev Air Tours is gratefully acknowledged. Special thank is due to their representative, Edit Omaisiz who contributed a lot to the success of the non-scientific arrangements.

The understanding attitude of the participants at a large extent to run the conference smoothly. Thanks to all of you

Dr. Tibor Nemetz, General Chair

June 1992

Program Chair's Report on the Eurocrypt'92

May 24-28, 1992, Balatonfüred, Hungary

What was special at Eurocrypt'92?

- For the first time, Eurocrypt'92 was held in an Eastern European country (Actually, that is old terminology. From our tour guide we learned that Hungary is in the center of Europe).
- For the first time, the General Chair and the Program Chair were based in different countries.
- The Program Committee managed to settle the final program without ever meeting.
- For the first time, a Panel discussion was organized, entitled "The Eurocrypt'92 Controversial Issue: Trapdoor Primes and Moduli".

The Submissions

We had a total of 88 regular submissions. The high quality of the submissions is illustrated by the fact that 54 of them (more than 60%) had an overall positive evaluation. But for the final program we could only accept 35 (40%) of the submissions. We also made an effort to balance the program to make it attractive to a large audience. The following list gives the number of submissions per country.

Australia	4	Austria	1
Belgium	3	Canada	5
China	2	Denmark	3
Finland	1	France	7
Germany	12	Ireland	1
Israel	1	Italy	3
Japan	13	Russia	1
Saudi Arabia	1	Spain	1

Sweden	2	Switzerland	4
The Netherlands	3	Turkey	2
UK	2	USA	14
Yugoslavia	2		

Only the current mailing address of the person who submitted the paper was taken for the evaluation. The fact that some joint papers had authors from different countries, or that an author submitted a paper from a different address than the usual one were not taken into account. Nevertheless, the figures give a general idea about the ongoing research activities in cryptology.

The Program Committee

From the Call for Papers and the Conference Announcement the official Program Committee is known. However, the Program Committee members were encouraged to obtain as much help as possible within their respective environments. Most of the members did so which caused the "real" Program Committee of Eurocrypt'92 to consist of 46 people. Here is the list of all those people (that I know of) who helped during the refereeing phase.

Brandt, Brickell, Charpin, Crepeau, Csirmaz, Damgaard, Denes, Desmedt, Feigenbaum, Fell, Fujioka, Golic, Helleseth, Itoh, Joux, Kenyon, Koyama, Kurosawa, Landrock, Matsui, Matsumoto, McCurley, Merritt, Miyaguchi, Miyaji, Morain, Morita, Nemetz, Odlyzko, Ohta, Okamoto, Quisquater, Sako, Sakurai, Santha, Seberry, Shamir, Simmons, Staffelbach, Stern, Tanaka, Vajda, Vallee, Yang, Yung, Rueppel.

My thanks go to all these colleagues for the time and effort they have invested to make Eurocrypt'92 a success.

One of the goals of the program committee was to settle the program without ever having a joint meeting. Therefore, disputes had to be resolved by electronic mail. The burden was considerable, more than 400 email messages passed through my office during the first 4 months of 1992. But somehow, the need to discuss critical issues by email seems to have had a positive effect. It was a pleasure to see that we reached complete agreement on the program.

The Rump Session, this time held more in the spirit of a recent results session, was chaired by Laszlo Csirmaz. There were 12 presentations, some of which will be included in the final Proceedings.

The Panel Discussion

The Panel consisted of seven members (for obvious reasons a prime number), which were:

Yvo Desmedt, University of Wisconsin
 Peter Landrock, Aarhus University
 Arjen Lenstra, Bellcore
 Kevin McCurley, Sandia National Laboratories
 Andrew Odlyzko, AT&T Bell Laboratories
 Rainer Rueppel, R³ Security Engineering
 Miles Smid, National Institute of Standards and Technology

The Panel was chaired by Rainer Rueppel. The topic was mainly motivated by the public discussion on the proposed DSS.

The hope was that Eurocrypt'92 would allow for a less emotional treatment of the subject (as compared to the discussion in the US). The Panel was organized in such a way that each of the members had a time slot of at most 10 minutes to make a personal statement. After the series of 7 statements an open discussion followed. In the end, the discussion turned out to be not as controversial as expected.

Regarding the DSS, NIST's reaction to allow for primes of up to 1024 bits took away much of the criticism raised during the period for comments.

Finally, I would like to thank the General Chair, Tibor Nemetz, and the local team for a smoothly organized and wonderfully situated Eurocrypt'92. It was a pleasure to serve as program chair of Eurocrypt'92. The wide support and help that I obtained are an unforgettable experience.

June 1992

Rainer A. Rueppel
 Program Chair, Eurocrypt'92

CRYPTO'92 - UPDATE

August 16-20 - Santa Barbara, CA

July 8, 1992

Dear Colleague:

Thank you for your registration to CRYPTO '92. You may find the information that follows of use while preparing for your trip and during the conference.

Program and activities: Special thanks to Ernie Brickell, Program Chair, and the Program Committee for preparing an excellent program. The program includes 13 sessions and 40 talks, 2 of which are invited. Technical sessions this year will be held in the Lotte Lehmann Concert Hall. The Rump and Poster Sessions will take place in the University Center Pavillion. A schedule of the talks is attached.

Rump Session: The rump sessions at the Crypto conferences have become unmanageable. There have been too many papers and too little time. The CRYPTO'92 program committee has therefore decided to institute long overdue drastic changes to this time-honored tradition.

Papers will be accepted for the RUMP *only if* they meet one of the following criteria:

1. The presentation is designed with the primary purpose of its comedy effect.
2. The paper was not submitted for the regular program, but had it been submitted, it would have been accepted without question.
3. The presentation is on a controversial topic of current interest to the cryptographic community and the presenter is prepared for hecklers from the audience.

Abstracts for presentations of Type 1 and 3 should be given to Whit Diffie before noon on Monday, August 17. Acceptance standards for Type 2 papers will be even higher than for papers in the regular program. To attempt to get a Type 2 paper accepted, please send 4 copies to the program chairman, Ernie Brickell, by July 31. The Type 2 papers that are accepted will be considered for inclusion in the Springer Proceedings. Addresses for Ernie Brickell: phone (505)-845-7655; fax (505)-845-7442; email efbrick@cs.sandia.gov

Regular mail

Ernie Brickell, Crypto'92
Dept. 1423
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185

Express mail

Ernie Brickell, Crypto'92
Dept. 1423
Sandia National Laboratories
1515 Eubank, SE
Albuquerque, NM 87123

Poster Session: In order to accommodate papers that would normally have been presented in the rump session (e.g. product announcements, new results, papers that did not quite make the regular program) we will have a poster session. The poster session will be held on Tuesday night immediately after the rump session if the rump session is as short as we expect it to be. Otherwise we will have the posters available during the day outside of the conference room.

Any member of the program committee can accept a paper for the poster session. To get a paper accepted, just send it to some member of the program committee before the conference, or show it to a member of the program committee at the conference. The only criterion will be that the work should be new and correct. If the number of papers submitted to the poster sessions gets too large (> 60), then we will stop accepting papers. Papers at the poster sessions will not be included in the Proceedings.

For the poster session, we will have available several large poster boards. Each person will be given enough space to put up 12 standard size pieces of paper. Do not just put up the complete text of a paper, because there will not be enough time to read the whole paper. Paper copies of viewgraphs which summarize results would be much better. Titles should be quite large, and all of the remaining text should be fairly large. Please include an address where people could write if they wanted a copy of your paper.

Registration and arrival instructions: Registration will be held in the Santa Rosa Hall from 4:00 to 8:00pm Sunday, August 16. A registration desk will also be set up on Monday morning at the Lotte Lehman Concert Hall, where the technical sessions will be held. A map of UCSB campus is attached. If you arrive by car, you must obtain a temporary parking permit when you enter the campus (see below). Those arriving at Santa Barbara airport Sunday afternoon can take the free UCSB shuttle to campus. Just call the Santa Rosa desk (tel 893-2772) and ask for a ride. A summary of travel information is attached.

Accommodations and meals: Participants who purchased the room and board package will stay on campus in Santa Rosa Hall, and will eat meals in De La Guerra Commons (cafeteria style, all you can eat). Rooms in Santa Rosa have no telephones, clocks, or radios, and bath facilities are shared. You may wish to bring a bathrobe and an alarm clock. You can check in after noon Sunday, and you should check out before 3:00pm Thursday. Keys must be returned at check-out; a \$28.00 fee will be charged for lost keys. Those arriving early or staying after the conference will need to make arrangements for off-campus lodging, since there are no general provisions for staying in the dormitory. Those not staying in the dormitory may buy individual meal tickets (cash only) preferably during registration, but tickets may be purchased also at De La Guerra Commons. A limited number of barbecue tickets will also be available. Our registration fee includes one barbecue ticket.

Parking on Campus: Anyone parking on campus must have a permit, and parking restrictions are strictly enforced. If you have a car, you should obtain a temporary parking permit at the campus gate when you first enter the campus. If you are staying on campus, you will receive at registration a complimentary permit good for the duration of the conference. If you are staying out of campus a charge of \$3.00 per day will be made for a parking permit. The permit should remain attached to your car.

Dress: Casual dress is appropriate for the entire conference. Daytime high temperatures are usually 65°F-85°F (18°C-30°C), and evening temperatures are usually 50°F-70°F (11°C-21°C). Temperatures during the beach barbecue will seem colder if it is windy, and a light jacket is recommended.

Smoking: UCSB prohibits smoking inside any buildings, with the exception of individual dormitory rooms. Smoking is allowed in outdoor areas, including breezeways and patios.

Messages: Messages for participants will be accepted and posted in Santa Rosa Hall. The telephone number for this service is (805)-893-2772.

Safety: Participants should take great care not to walk on designated bicycle paths on campus. If an earthquake occurs while you are in a building, you should take cover under a desk or table, or sit or stand against an inside wall or doorway. Stay away from glass such as windows and mirrors. When the earthquake stops, leave the building, and remain outside until you are informed it is safe to return.

Alcoholic beverages are served at the cocktail parties, rump session, and beach barbecue. If you wish to drink, please stay on campus so that you will not need to drive. If you stay off campus and must drive, please drink soft drinks.

Tar: When walking on the beaches in Santa Barbara, be aware of the tar. If you choose to walk on the beach, you may wish to bring some baby oil to help remove the tar.

I am looking forward to seeing you at CRYPTO '92!

Spyros S. Magliveras
General Chair

Dept. of Computer Science and Engineering
University of Nebraska -- Lincoln
Lincoln, NE 68588-0115

(402)-472-5005
(402)-472-7767 (fax)
spyros@helios.unl.edu

CRYPTO '92 - Travel Information

From north or south by car:

UCSB is approximately 10 miles north of the city of Santa Barbara, and approximately two hours north of Los Angeles by U.S. 101. The exit from U.S. 101 to the campus is well marked.

From Santa Barbara airport to campus by shuttle:

UCSB shuttle:

- no charge
- will pick you up from baggage area upon request. Please call 893-2772.
- Sunday and Thursday afternoons only
- information: (805)-893-2772

From Los Angeles airport to Santa Barbara by bus:

- "Super Shuttle" buses
 - one way: approximately \$50
 - arrange upon arrival at airport
- Santa Barbara "Air Bus"
 - to Sheraton Santa Barbara
 - one way: \$33 (\$28 if prepaid 24 hours in advance)
 - round trip: \$57 (\$52 if prepaid 24 hours in advance)
 - departs 8:00 and 10:30am, 1:00, 3:30, 6:00, 8:30, and 11:00pm
 - 2-hour trip
 - information: (805)-964-7759

From Los Angeles train station to Santa Barbara train station by train or bus:

- Amtrak train/bus
 - one-way: \$20
 - round trip: \$25
 - train departs 8:15 am, 8:00 pm ; bus departs 12:50 pm, 4:45 pm and 9:15 pm
 - 2-1/2-hour trip (train), between 3 and 4 hour trip (bus)
 - information: (800)-USA-RAIL (800-872-7245)
- UCSB shuttle does not serve the train station. Taxis are readily available.

CRYPTO'92 - Preliminary Schedule

August 16-20 - Santa Barbara, CA

CRYPTO'92 is the twelfth in a series of workshops on cryptology, and is sponsored by the International Association for Cryptologic Research, in cooperation with IEEE Computer Society Technical Committee on Security and Privacy, the Department of Computer Science & Engineering of the University of Nebraska - Lincoln, and the Computer Science Department of the University of California, Santa Barbara.

The following people served on the Program Committee:

Ernie Brickell (Chair, Sandia National Laboratories)
Ivan Damgard (Aarhus University, Denmark)
Oded Goldreich (Technion, Israel)
Burt Kaliski (RSA Data Security),
Joe Kilian (NEC),
Neal Koblitz (University of Washington),
Ueli Maurer (ETH, Switzerland),
Chris Mitchell (Royal Holloway, England),
Kazuo Ohta (NTT, Japan),
Steven Rudich (Carnegie Mellon),
Yacov Yacobi (Bellcore).

All sessions except for the rump and poster sessions will be held in the Lotte Lehman Concert Hall. The rump and poster sessions will be held at the UCen (University Center).

Sunday, August 16, 1992

4:00--8:00 pm & Registration -- Santa Rosa

5:30--6:30 pm & Dinner

7:00--10:00 pm & Cocktail Party -- Santa Rosa Hall

Monday, August 17, 1992

7:00--8:00 am Breakfast

Session 1: Digital Signatures and Identification I - Chair: Ivan Damgard8:30--8:50 am *Provably Unforgeable Signatures*, David Chaum, Jurjen Bos, (CWI - Amsterdam, The Netherlands)8:55--9:15 am *New Constructions of Fail-Stop Signatures and Lower Bounds*, Birgit Pfitzmann (Universitat Hildesheim, Germany), Eugene van Heijst (CWI, The Netherlands), Torben Pryds Pedersen (Aarhus Universitet)9:20--9:40 am *Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes*, Taksuaki Okamoto (NTT Laboratories, Japan)9:45--10:05 am *An Efficient Digital Signature Scheme Based on an Elliptic Curve over the ring Z_n* , Tatsuaki Okamoto, Atsushi Fujioka, Eiichiro Fujisaki (NTT Laboratories, Japan).

10:05--10:35 am Break

Session 2: The Digital Signature Standard - Chair: Ernie Brickell10:35--10:55 am *Designing and Detecting Trapdoors for Discrete Log Cryptosystems*, Daniel M. Gordon (University of Georgia, USA)11:00--11:55 am *NIST Cryptographic Standards: Present and Future Trends* Miles Smid (Invited talk)

12:00--1:00 pm Lunch

Session 3: Applications and New Problems - Chair: Burt Kaliski1:30--1:50 pm *Wallet Databases with Observers*, Torben Pryds Pedersen, (Aarhus University, Denmark), David Chaum (CWI, The Netherlands)1:55--2:15 pm *Making Electronic Refunds Safer*, Rafael Hirschfeld (MIT, USA)2:20--2:50 pm *Fair Public-Key Cryptosystems*, Silvio Micali (MIT, USA)2:55--3:15 pm *Pricing via Processing or Combating Junk Mail*, Moni Naor, Cynthia Dwork (IBM Almaden, USA)

3:15--3:45 pm Break

Session 4: Secret Sharing I - Chair: Chris Mitchell3:45--4:05 pm *On the Information Rate of Secret Sharing Schemes*, Alfredo De Santis, C. Blundo, L. Gargano, U. Vaccaro (Università di Salerno, Italy)4:10--4:30 pm *New General Lower Bounds on the Information Rate of Secret Sharing Schemes*, D. R. Stinson (University of Nebraska, USA)4:35--4:55 pm *Universally Ideal Secret Sharing Schemes*, Benny Chor, Amos Beimel, (Technion, Israel)

5:30--6:30 pm Dinner

7:00--10:00 pm Cocktail Party -- Santa Rosa Hall

Tuesday, August 18, 1992

7:00--8:00 am Breakfast

Session 5: Theory I - Chair: Joan Boyar8:30--8:50 am *Perfect Zero-Knowledge Arguments for NP can be based on General Complexity Assumptions*, Moti Yung (IBM J.T. Watson, USA), Moni Naor (IBM Almaden, USA), Rafail Ostrovsky (MIT, USA), Ramarathnam Venkatesan (Bellcore, USA)8:55--9:15 am *Low Communication 2-Prover Zero-Knowledge Proofs for NP*, Joe Kilian, (NEC, USA), Cynthia Dwork (IBM Almaden, USA), Uri Feige (IBM T.J. Watson, USA), Moni Naor, Muli Safra (IBM Almaden, USA)9:20--9:40 am *Non-Interactive Zero-Knowledge Proofs and Invariant Signatures are Equivalent*, Rafail Ostrovsky, Shafi Goldwasser (MIT, USA)9:45--10:05 am *On the Discrepancy between Serial and Parallel of Zero-Knowledge Protocols*, Kouichi Sakurai (Mitsubishi, Japan), Toshiya Itoh (Tokyo Institute of Technology, Japan)

10:05--10:35 am Break

Session 6: Cryptographic functions - Chair: Yacov Yacobi10:35--10:55 am *On the Design of SP Networks from an Information Theoretic Point of View*, S. E. Tavares, M. Sivabalan, L. E. Peppard (Queen's University at Kingston, Canada)11:00--11:20 am *Partially-bent Functions*, Claude Carlet (INRIA, France)**Session 7: Digital Signatures and Identification II - Chair: Yacov Yacobi**11:25--11:45 am *Practical Approaches to Attaining Security Against Adaptively Chosen Ciphertext Attacks*, Yuliang Zheng, Jennifer Seberry (University of Wollongong, Australia)11:50--12:10 pm *On the Security of the Permuted Kernel Identification Scheme*, Henri Gilbert, Thierry Baritaud, Mireille Campana (Centre National d'Etudes des Telecommunications, France)

12:15--1:00 pm Lunch

1:00--5:30 pm Free Afternoon

5:30--6:30 pm Dinner

7:00 pm -- ? Rump Session -- University Center

Wednesday, August 19, 1992

7:00--8:00 am Breakfast

Session 8: Computational Number Theory - Chair: Neal Koblitz

- 8:30--8:50 am *Massively Parallel Computation of Discrete Logarithms*, Daniel M. Gordon, (University of Georgia, USA), Kevin S. McCurley (Sandia National Laboratories, USA)
- 8:55--9:15 am *A Quadratic Sieve on the n-Dimensional Cube*, Rene Peralta (University of Wisconsin, USA)
- 9:20--9:40 am *Efficient Multiplication on Certain Nonsupersingular Elliptic Curves*, Othmar Staffelbach (Gretag Data Systems, Switzerland), Willi Meier (HTL, Switzerland)
- 9:45--10:05 am *Speeding Up Elliptic Cryptosystems by Using a Signed Binary Window Method*, Kenji Koyama, Yukio Tsuruoka (NTT, Japan)
- 10:00--10:35 am Break
- 10:35--10:55 am *On Generation of Probable Primes by Incremental Search*, Jorgen Brandt, Ivan Damgard (Aarhus University, Denmark)

Session 9: Cryptography Education - Chair: Neal Koblitz

- 11:00--11:50 am *Kid Krypto (Computer Science for Children)*, Mike Fellows (Invited Talk)
- 12:00--1:00 pm Lunch

Session 10: Theory II - Chair: Steve Rudich

- 1:30--1:50 pm *On Defining Proofs of Knowledge*, Mihir Bellare (IBM T.J. Watson, USA) Oded Goldreich (Technion, Israel)
- 1:55--2:15 pm *Public Randomness in Cryptography*, Amir Herzberg (IBM T.J. Watson, USA), Michael Luby (International Computer Science Institute, USA)
- 2:20--2:50 pm *Necessary and Sufficient Condition for Collision-Free Hashing*, Alexander C. Russell (MIT, USA)
- 2:55--3:15 pm *Verifying Cryptographic Tools*, Moti Yung, Mihir Bellare (IBM T.J. Watson, USA)
- 3:15--3:45 pm Break

Session 11: Key Distribution - Chair: Joe Kilian

- 3:45--4:05 pm *Protocols for Secret Key Agreement by Public Discussion Based on Common Information*, Ueli M. Maurer (Institute for Theoretical Computer Science, Switzerland)
- 4:10--4:30 pm *Perfectly-Secure Key Distribution for Dynamic Conferences*, Moti Yung (IBM T.J. Watson, USA), C. Blundo, A. De Santis, U. Vaccaro (Università di Salerno, Italy), A. Herzberg, S. Kuttan (IBM T.J. Watson, USA)

4:35--6:00 pm IACR Business meeting

6:00--9:00 pm Beach barbecue -- Goletta Beach

9:10--11:00 pm Possible Movie : *Sneakers* -- Santa Rosa Hall

Thursday, August 20, 1992

7:00--8:00 am Breakfast

Session 12: DES - Chair: Ueli Maurer

- 8:30--8:50 am *Differential Cryptanalysis of the Full 16-round DES*, Eli Biham (Technion, Israel), Adi Shamir (Weizman Institute of Science, Israel)
- 8:55--9:15 am *Iterative Characteristics of DES and s^2 DES*, Lars Ramkilde Knudsen (Aarhus University, Denmark)
- 9:20--9:40 am *Strong Evidence that DES is not a Group*, Keith W. Campbell, Michael J. Wiener (Bell-Northern Research, Canada)
- 9:45--10:05 am *A High-Speed DES Implementation for Network Applications*, Hans Eberle (Digital Equipment Corporation, USA)
- 10:05--10:35 am Break

Session 13: Secret Sharing II - Chair: Kazuo Ohta

- 10:35--10:55 am *Threshold Schemes with Disenrollment*, Agnes Hui Chan (MITRE, USA), Bob Blakley (IBM Austin, USA), G. R. Blakley (Texas A&M University, USA), James L. Massey (Swiss Federal Institute of Technology, Switzerland)
- 11:00--11:20 am *Non-existence of Homomorphic General Sharing Schemes for Some Key Spaces*, Yair Frankel, Yvo Desmedt (University of Wisconsin, USA), Mike Burmester (University of London, England)
- 11:25--11:45 am *An 1-Span Generalized Secret Sharing Scheme*, Lein Harn, Hung-Yu Lin (University of Missouri -- Kansas City, USA)
- 12:00--1:00 pm Lunch
- 1:00 pm Adjourn

CRYPTO '92 - Registration Form
The Deadline for Registration is JULY 10, 1992

Last Name: _____ First Name: _____ Sex: (M) ___ (F)___

Affiliation: _____

Mailing Address: _____

Electronic Mail: _____

Telephone: (____) _____

Alternate Telephone: (____) _____

Payment of the conference fee entitles you to membership in the International Association for Cryptologic Research for one year at no extra charge. With membership in the IACR you are entitled to receive 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.

Conference fee :	Regular (\$218)	\$ _____
	Attended Eurocrypt '91, Brighton (\$178)	\$ _____
	Full time student (\$138)	\$ _____
Room and Board :	Single room (\$275 per person)	\$ _____
	Double room (\$220 per person)	\$ _____
	Roomate: _____	
Barbecue tickets (\$20 each)		\$ _____
	(one is included in the room and board charge)	
Total funds enclosed:		\$ _____

Fees: Payment must be in U.S. funds, by check drawn on a U.S. bank or by international money order payable in U.S. funds, PAYABLE TO CRYPTO '92. Payment should be mailed to:

Spyros S. Magliveras, CRYPTO '92
Dept of Computer Science and Engineering
University of Nebraska - Lincoln
Lincoln, NE 68588-0115
U.S.A.

A very limited number of stipends are available to those unable to obtain funding. Applications for stipends should be sent to the general chairman before June 5, 1992. The Deadline for Registration is July 10, 1992

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. However, mention CRYPTO '92 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 \$79, Double \$84, University rate \$65.00 for single or double. Call Ms Sheri Pang at (805)-967-3200, or toll-free at (800)-350-3614.

Turnpike Lodge : 4770 Calle Real, Santa Barbara, 93110. Regular rates: Single \$78, Double \$88, University rates \$68 (single), \$78 (double). Call Mr. 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 Mr. Bill Connor at (805)-964-3596.

The Sandman Inn : 3714 State St., Santa Barbara, CA 93105. Regular rates: Single or Double \$84, \$94 for king-size, University rate \$65. Call Ms Christina Ortwein 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 Street, Santa Barbara, CA 93105. Regular rates: \$106 - \$112 for two people, University rates \$96 - \$102 for two people. Call Ms Barbara Thomson 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, call for University rates. Contact Ms Carol Wolford at (805)-682-7550 or toll-free at (800)-526-2282.

For further information, contact the general chair:

Spyros S. Magliveras, CRYPTO '92
Dept. of Computer Science and Engineering
University of Nebraska - Lincoln
Lincoln, NE 68588-0115
U.S.A.

AUSCRYPT'92

(Sunday 13 December to Wednesday 16 December, 1992)

CALL FOR PAPERS

The Second AUSCRYPT Conference, sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Information Security Research Centre (ISRC) and the School of Mathematics, Queensland University of Technology (QUT), Brisbane, Queensland and the Computer Science Department of the University of Wollongong, Wollongong, N.S.W. will be held on the campus of Somerset College, Mudgeeraba, (Gold Coast), Queensland from Sunday 13 to Wednesday 16th December, 1992. Original research papers and technical expository talks are solicited on all practical and theoretical aspects of cryptology. It is anticipated that some talks may also be presented by special invitation of the program committee.

Instructions for authors: Authors are requested to send 12 copies of a detailed abstract (not a full paper) by 11 September, 1992, to the Program Chair at the address given below. In order to receive consideration by the Program Committee, submissions must arrive on time or be postmarked no later than 4 September, 1992 and be sent by airmail. It is requested 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 developments directed to the specialist should follow as needed.

Abstracts which have been submitted to other conferences that have proceedings are not eligible for submission to AUSCRYPT.

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

Authors will be informed of acceptance or rejection in a letter mail on or before 1 November, 1992. Accepted papers may then be submitted in extended form. A compilation of all accepted abstracts will be available at the conference. Authors of accepted papers will be given until 15 November, 1992, to submit revised versions for this compilation.

Complete conference proceedings will be submitted to Springer-Verlag's Lecture Notes in Computer Science series for publication at a later date.

The Program Committee consists of: Mike Burmester (UK), Yvo Desmedt (Milwaukee, USA), Hideki Imai (JAPAN), Svein Knapskog (NORWAY), Rudi Lidl (Tasmania, AUSTRALIA), John Loxton (Macquarie, AUSTRALIA), Tsutomu Matsumoto (JAPAN), Josef Pieprzyk (Wollongong, AUSTRALIA), Rei Safavi-Naini (Wollongong, AUSTRALIA).

The Organising Committee consists of Chairman / Bill Caelli (QUT, Australia), Vice-Chairman -Ed Dawson (QUT, Australia), Ian Graham (ERACOM, Australia), Eleanor Crosby (TURNIX, Australia), Barry Arnison (Somerset College, Australia). The conference is being organised by the Office of Educational Services (OES) of the Queensland University of Technology.

Send abstracts to the Program Chair:

Jennifer Seberry
Centre for Computer Security Research
Department of Computer Science
University of Wollongong
WOLLONGONG NSW 2500
AUSTRALIA

Internet: jennie@cs.uow.edu.au

For other information contact the
General Chair:

Bill Caelli
Information Security Research Centre
Queensland University of Technology
GPO Box 2434
BRISBANE QLD 4001
AUSTRALIA

Internet: w.caelli@qut.edu.au

AUSCRYPT'92

13 - 16 DECEMBER 1992

GENERAL INFORMATION

Program. Auscrypt'92 is the second conference and workshop on cryptology to be held in Australia. The conference is sponsored by the International Association for Cryptologic Research (IACR), in cooperation with the Information Security Research Centre (ISRC) and the School of Mathematics, Queensland University of Technology (QUT), Brisbane, Queensland and the Computer Science Department of the University of Wollongong, Wollongong, N.S.W. The program will cover all abstracts 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 also be a "Rump Session" on Tuesday evening, 15 December, (before the Conference Dinner) for informal presentations. Facilities will also be provided for attendees to demonstrate items of cryptographic interest. If you wish to present a poster or demonstration please contact Bill Caelli, the General Chair, so that your needs may be attended to. (Both IBM compatible PCs under DOS and Apple Macintosh computers are available.) The social program will include hosted cocktail parties on Sunday and Wednesday nights, a conference dinner on Tuesday evening and an optional excursion to a major Gold Coast attraction on Monday 14th December. The cocktail parties and dinner are included in the conference fee. Additional tickets for all social functions are available as indicated on the registration form.

Conference facilities. The conference will be held on the campus of Somerset College, Mudgeeraba, situated in the Gold Coast hinterland. The conference has been timed for the week before the State Schools Summer Vacation begins in order to take advantage of lower accommodation costs and better availability. Please book your own accommodation or take advantage of the booking service, as detailed separately. Please return the Accommodation Booking Form to the accommodation booking service at the address given. The Registration Form needs to be separately sent to QUT at the address given for registrations. (The registration form also asks if you are using the Accommodation Booking Service to inform the Organising Committee for bus allocation, etc.) Parking at Somerset College is free. Somerset College is a ten year old independent co-educational school. The facilities of the college will be available to attendees, including use of the library, photocopying facilities, souvenir/stationary shop, computer laboratories, etc. There will be no students present during conference week. Limited spaces will be available in the Woodlands Pre-school for child-minding for children 2 - 5 years old, from 7.45am to 5.45pm during the conference. This school is on land adjoining Somerset College. Please contact the General Chair as soon as possible if you contemplate placing a child during your stay. Child-minding fees are \$25.00 per day per child and are your responsibility. Places are extremely limited and early bookings are needed.

Travel information. Somerset College is located in the Gold Coast Hinterland some 8 Kilometres to the West of Burleigh Heads. It is some 90km south of Brisbane, the location of the nearest international airport and 30km from Coolangatta/Gold Coast airport, the local national airport. Bus transfers from Brisbane or Coolangatta Airports to the Gold Coast area and to your accommodation may be arranged by your travel agent or on arrival. All major Rental Car agencies operate at both airports. Full information on bus / limousine transfers and related arrival/departure details will be provided with the registration kit.

A bus service will be arranged to convey participants from their accommodation to Somerset College. Please indicate on the registration sheet if you will need to use the bus.

Registration. All interested parties are invited to register. Pre-registration is required. To register, fill out the attached registration form and return to the address on the form along with payment in full before Friday, 13 November, 1992. The conference fee includes participation in the program, lunches, morning and afternoon teas, cocktail parties and dinner, as well as membership to the IACR for 1993.

Pre and Post Conference Tours. The Gold Coast is the premier tourist centre in Australia and numerous tours and holiday attractions are available. Your travel agent should be able to supply you with a broad range of interesting tours in the region, around the State of Queensland, including the Great Barrier Reef, as well as further afield in Australia.

(The period from around December 18 till late January is Australia's peak holiday season and early bookings are needed. Thus tours before the conference, i.e. before 13 December, may be easier to arrange and will be less costly.)

AUSCRYPT'92 - REGISTRATION FORM.
 THE DEADLINE FOR REGISTRATION IS 13 NOVEMBER 1992.

Last name: _____ First name: _____ Title: _____

Affiliation: _____

Mailing address: _____

Electronic mail: _____

Telephone: (Country) _____ (City) _____ (No) _____

AlternatePh: (Country) _____ (City) _____ (No) _____

FACSIMILE: (Country) _____ (City) _____ (No) _____

Payment of the conference fee entitles you to membership of the International Association for Cryptologic Research (IACR) for one year (calendar year 1993). With membership in the IACR you are entitled to receive a subscription to the Journal of Cryptology, published by Springer-Verlag, at no extra charge. (Those who attend Eurocrypt'92 and/or Crypto'92 would already be members and thus may opt for the lesser conference fee.)

.....

Do you wish to be an IACR member? Yes No

.....

Conference Fee : Regular Fee	(\$ 415 - Aust)	\$ _____
Attended Eurocrypt'92 or Crypto'92	(\$ 365 - Aust)	\$ _____
Full-time Student	(\$ 195 - Aust)	\$ _____

ADDITIONAL TICKETS FOR SOCIAL FUNCTIONS

Welcome Reception (Sunday 13 Dec)	(\$ 15 - Aust each)	\$ _____
Conference Dinner (Tuesday 15 Dec)	(\$ 50 - Aust each)	\$ _____
Farewell Drinks (Wednesday 16 Dec)	(\$ 15 - Aust each)	\$ _____

TOTAL FEES ENCLOSED \$ _____

PAYMENT : Payments must be made in Australian Dollars (\$1 Aust = \$0.75 U.S. approx) by cheque drawn on an Australian bank or by international bank cheque made payable to "AUSCRYPT'92". Payment by major credit card is also acceptable as detailed below. Payments with the appropriate registration and accommodation forms should be sent to:


AUSCRYPT'92 Secretary,
Office of Educational Services,
Queensland University of Technology,
G.P.O. Box 2434,
BRISBANE QLD 4001
AUSTRALIA

Fax : +61 - 7 - 864 3529 (International)
 07 - 864 3529 (National)
 Phone: +61 - 7 - 864 2822 (International)
 07 - 8642822 (National)

I have taken advantage of the **Accommodation Booking Service** Yes No

I need assistance with child minding facilities Yes No

I will be using the bus service to / from Somerset College Yes No

AMOUNT DUE \$ - - - - -	
<input type="checkbox"/> I enclose cheque - make payable to QUT & mark 'not negotiable'	
<input type="checkbox"/> Charge to my credit card:	Bankcard <input type="checkbox"/>
	MasterCard <input type="checkbox"/>
	Visa <input type="checkbox"/>
	
CARD HOLDER'S NAME: _____	
ADDRESS: _____	
SIGNATURE: _____	
EXP DATE: _____	

ACCOMMODATION BOOKING FORM

Name: _____
(Title first, Surname/family name in capitals)

Address: _____

P/code: _____ Phone: _____ Fax: _____

e-mail: _____

Please tick the options below as appropriate.

1. **PREFERRED CONFERENCE ACCOMMODATION VENUE:** (Air conditioned, single, double or three person units, pool, restaurant, bar (at hotel prices). Prices are quoted on a per unit basis.

- Single \$50.00 per night.
 Twin/ double \$50.00 per night.
 Triple share \$75.00 per night

No. of people: _____. Nights require: (3)-13/15 December, or: other _____

Please arrange shared accommodation for me with other or other of the same sex. I am male female

2. **FIVE STAR HOTEL** Single with breakfast \$150.00 per night
 Double with breakfast \$150.00 per night

No. of people: _____. Nights require: (3)-13/15 December, or: other _____

3. **LUXURY APARTMENT ON THE BEACH.** 2 bedroom, 2 bathroom, lounge, kitchen, laundry, pool, tennis court, barbecue. Sleep 4 people. (Specify 1 double, 2 singles or 4 singles, etc). 7 nights, \$700.00 (12 - 18 December inclusive) per apartment. Other periods by negotiation, please indicate _____

4. **BUDGET MOTEL.** Usual good Gold Coast standard, TV, pool, etc. Single \$35.00 per night
 Twin share \$35.00 per night
 Triple share \$45.00 per night

No. of people _____ Nights required: 13 - 15 December, or other: _____

I enclose a deposit of \$Aust 50.00 per person to secure accommodation. This must be in the form of a cheque drawn on an Australian bank or by international bank cheque made payable to **ACCOMMODATION BOOKINGS GOLD COAST**. Major credit cards are also acceptable. Please complete the authorisation below.

Credit Card Payment: Deposit - Total \$ Aust _____ (\$Aust 50.00 per person)

Card no. Expiry date _____

Card (circle): VISA MasterCard Bankcard AMEX Diners Other - Please identify.

Signature: _____

Please return this form to:
**ACCOMMODATION BOOKINGS GOLD COAST
ATTN : NOELLE LUCAS
P O BOX 1477
BROADBEACH QLD 4218 AUSTRALIA**

Phone: +61 - 75 - 385 269 - International - or 075 - 385 269 - National.
Facsimile: +61 - 75 - 315 096 - International - or 075 - 315 096 - National.

DEADLINE: 13 NOVEMBER 1992. PLEASE BOOK ACCOMMODATION EARLIER IF POSSIBLE: THIS IS HOLIDAY SEASON ON THE GOLD COAST!



EUROCRYPT '93

May 24-27, 1993
Hotel Ullensvang, Lofthus, NORWAY

A Workshop on the Theory and Applications
of Cryptographic Techniques

Sponsored by
the International Association for Cryptologic Research (IACR)

CONFERENCE ANNOUNCEMENT

Eurocrypt 'NN constitute a series of European conferences dedicated to the theory and applications of cryptographic techniques. The program includes topics like symmetric and asymmetric ciphers, authentication, protocols, secure transactions, signatures, sequences and complexity, hardware and software solutions, security of telecommunication systems and computer networks.

EUROCRYPT '93 will take place at Hotel Ullensvang in Norway. The conference site is beautifully located in the village of Lofthus in the heart of Norway's Fjord District. All activities will take place at the hotel which provides excellent conference facilities. The hotel is situated by the shore of the Hardangerfjord, which is one of the longest fjords in Norway. This offers excellent possibilities for interesting walks in the near surroundings as well as boating on a Norwegian fjord. This district is famous for cultivation of apples and the blossom should be at its peak during the conference.

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

CLIMATE

In May the temperature is expected to range from 15 to 20 degrees C in daytime.

ACCOMODATION

The accomodation will be shared between Hotel Ullensvang and Fjordhotel Kinsarvik. Cheaper accomodation for students will be provided.

Claude Crépeau, Editor

Département de Mathématiques et d'Informatique
École Normale Supérieure
45, rue d'Ulm
75230 Paris CEDEX 05
FRANCE

téléphone: +33 (1) 44.32.20.61
FAX: +33 (1) 44.32.20.80
email: crepeau@dmi.ens.fr

Editor-in-Chief

Gilles Brassard

Editors

Thomas A. Berson
Ernest F. Brickell
Johannes Buchmann
David Chaum
Don Coppersmith
Claude Crépeau
Ivan Damgård
Joan Feigenbaum
Oded Goldreich
Martin E. Hellman
David Kahn
James L. Massey
Andrew M. Odlyzko
Steven Rudich
Rainer A. Rueppel
Adi Shamir
Gustavus J. Simmons
Andrew C.-C. Yao

April 22, 1992

To all contributors,

The Journal announces a SPECIAL ISSUE on ZERO-KNOWLEDGE.

All authors with original results in that area are encouraged to submit papers for that special issue. Contributions should be sent to the special issue editor at the above address or by e-mail in \LaTeX format.

Please note that submissions for the special issue will be accepted until September 1st, 1992.

Happy writing!

Claude Crépeau
Editor

Abstracts of Recent Publications

TITLE: Principles for Designing Secure Block Ciphers and One-Way Hash Functions

AUTHOR: Yuliang Zheng

SUPERVISOR: Hideki Imai

UNIVERSITY: Division of Electrical and Computer Engineering,
Yokohama National University, JAPAN

DATE THE DEGREE WAS GRANTED: March 27, 1991

ABSTRACT: This thesis is concerned with issues of designing secure (secret-key) block ciphers and constructing one-way hash functions. Both block ciphers and one-way hash functions are indispensable to secure information systems built on cryptographic techniques. With a block cipher, we can safeguard our important information transmitted over insecure communication networks. And with a one-way hash function, we can safely compress very long messages into relatively short ones to improve the overall efficiency of an information system or to detect unauthorized modifications to these messages.

The thesis consists of two parts. Part 1 deals with designing secure block ciphers and Part 2 with constructing one-way hash functions. The outlines of the two parts are as follows.

In Part 1, we first prove an impossibility result on constructing pseudo-random permutations from random functions, which is closely related to the design of secure block ciphers. Then we consider the problem of constructing block ciphers which have the following ideal properties:

1. The ciphers are provably secure.
2. Security of the ciphers does not depend on any unproved hypotheses.
3. The ciphers can be easily implemented with current technology.
4. All design criteria for the ciphers are made public.

It is currently unclear whether or not there really exists such an ideal block cipher. So to meet the requirements of practical applications, the best thing we can do is to construct a block cipher such that it approximates the ideal one as closely as possible. In this thesis, we make a significant step in this direction. In particular, we construct several block ciphers which have the above mentioned properties 2, 3 and 4 as well as the following one:

- 1'. Security of the ciphers is supported by convincing evidence.

In Part 2, we first reveal a duality between constructions of two basic cryptographic primitives, pseudo-random string generators and one-way hash functions. Applying the duality, we present a construction for universal one-way hash functions assuming the existence of one-way permutations. Using ideas behind the construction, we propose practical one-way hash functions, the fastest of which compress nearly $2n$ -bit long input into n -bit long output strings by applying only twice a one-way function.

Then we prove that universal one-way hash functions with respect to initial-strings chosen arbitrarily exist if and only if universal one-way hash functions with respect to initial-strings chosen uniformly at random exist. As an application of the result, we show that universal one-way hash functions with respect to initial-strings chosen arbitrarily can be constructed under the assumption of the existence of one-way quasi-injections.

Finally, we investigate relationships among various versions of one-way hash functions. We prove that some versions of one-way hash functions are strictly included in others by explicitly constructing hash functions that are one-way in the sense of the former but not in the sense of the latter.

Title: Applications of Cryptography for the Security of Database and Distributed Database systems

Author: Thomas Hardjono

Institution: University of New South Wales, Australia.

Supervisor: Prof. J. Seberry

Abstract:

This thesis presents an investigation into the applications of the techniques of cryptography for the security of centralized and distributed database systems. Three major schemes associated with cryptography are presented. The first is a multi-level encryption scheme based on the Rivest-Shamir-Adleman (RSA) cryptosystem, which can be applied to database systems. Each data item in the database is encrypted using keys associated with the sensitivity or security level of that data item. Each user is given a key derived from one of the set of decryption keys associated with each security level, corresponding to the encryption keys of the data items.

The second scheme is designed to be used for the encryption of data in distributed database systems. Each site in the distributed database system receives some secret information which is shared by all the legal sites. In addition, each site chooses its own secret parameters, which together with the shared information is used to encrypt data items at that site. The technique used in encryption allows encrypted data items to be decrypted during query processing with out too much overhead in terms re-encryption for secure data communications.

The third scheme represents an improvement on a previous idea on the encipherment of B-Trees in database systems for allowing encrypted records to be searched for effectively in the database. Some modifications to the original idea is presented in order to gain significant improvement in performance. The focal point of the improvement is a scheme which employs combinatorial structures to hide or disguise the search keys in the B-Tree based on combinatorial block designs. In this manner, only one decryption step is necessary at each B-Tree node during the traversal of the tree.

This thesis also investigates a possible solution to the hierarchical access control problem. The solution is given concretely in the form of three key generation schemes, followed by a discussion on the security of each scheme. The first scheme is based on pseudo-random functions and universal hash functions, and is proven to be weakly secure. The second scheme, which is shown to be strongly secure, is based on pseudo-random functions and the sibling intractable function family. The third scheme, based only on the sibling intractable function family is pragmatically secure. The problem of updates of the keys in the hierarchical organization is also considered. Although this thesis uses the solution only for the hierarchical access control problem, it is applicable to a wide range of situations and it may be a solution to a number problems relating to access control and key management in cryptography.

