FAX Message

Date: 2/6/95

To: IACR Board of Director Member

Company:

Fax Phone Number: 1-415-324-0120

CC:

From: G.B. Agnew IACR Newsletter Editor

Subject: Minutes of BoD meeting

# of Pages (including this cover sheet): 4

Message:

Dear Board Member

Sherry has asked me to pass along a copy of the minutes of our last meeting.
Unfortunately, I had trouble with the electronic version so we will resort to old fashion paper - sorry about the inconvenience and the delay.
Regards.
Gord.

If you do not receive all pages, please call back immediately.

Voice: Fax: Telex:

The International Association for Cryptologic Research (IACR)
Board of Directors Meeting, 21 August, 1994

The meeting of the IACR Board of Directors (herein referred to as the BOD) was called to order by the president, Peter Landrock at approximately 2:00 p.m. on 21 August, 1994. The following members were in attendance: officers: Peter Landrock, Ingemar Ingemarsson, Kevin McCurley, and Sherry Shannon; directors: Andy Clark, Gord Agnew, Gilles Brassard, Tom Berson, Hideki Imai, Scott Vanstone, Rainer Rueppel, Paul Van Oorschot, Jean-Jacques Quisquater, Whitfield Diffie, and Jimmy Upton (General Chair, Crypto '94). Absent were Jennifer Seberry, William Wolfowicz and Bob Blakley (Tom Berson has his proxy). (Note: proxies are not counted unless specifically voted.)

AGENDA, as proposed by Peter Landrock, was approved.

BOD MINUTES- EC '94: BOD approved the minutes as reported in the June 1994 IACR Newsletter.

CRYPTO '94 REPORT: Jimmy Upton presented a status of Crypto '94. At the time 325 people had pre registered.

EUROCRYPT '94 REPORT: Neither the financial report nor general report have been received. Peter Landrock has heard from William Wolfowicz, General Chair of EC '94, and a report will be ready by September.

QUESTIONNAIRE: An IACR members questionnaire has been prepared by Sherry Shannon and Ingemar Ingemarsson and will be presented by Peter Landrock to the members at the General Assembly meeting on Wednesday, 24 August. Responses and comments from the questionnaire are to be returned to Peter Landrock. Peter will present to the BOD at Eurocrypt '95.

EUROCRYPT '95 REPORT: EC '95 will be held in Saint Malo, France from 22 to 25 May, 1995. Louis Guillou, the Program Chair for EC '95 gave the report. The call for papers is ready and the papers must be received by 2 December, 1994. The authors will be notified by 23 January and final papers will need to be ready by 6 March.

Kevin McCurley, the IACR treasurer, still needs a budget from Francois Scanrabin, the General Chair, Plans are being made for around 300 attendees and it is anticipated that the fee and board will be around 2500 Francs. The BOD encouraged Louis to keep the fees as low as possible with plans to just break even.

General Guidelines to be sent by Sherry Shannon, mailing list and labels to be sent by Andy Clark and IACR logo to be sent by Jimmy Upton.

FUTURE CONFERENCES: Crypto '95 will be held in Santa Barbara, CA from 27 to 31 August, 1995. Stafford Travares is the General Chair and the BOD decided to ask Don Coppersmith to be the Program Chair (Don accepted).

Crypto '96 will be held in Santa Barbara, CA with dates to be determined. The Board decided to ask Richard Graveman to be the General Chair (Richard accepted). Program Chair will be decided later.

Eurocrypt '96 will be held in Zaragoza, Spain with dates to be determined. Jose Pastor is the General Chair. Ueli Maurer is the Program Chair.

For Eurocrypt '97, UK and Germany were mentioned as possibilities. Proposals are welcome from any country and should be prepared and sent to Peter Landrock for submission to the BOD at EC '95.

"In Cooperation with" Conferences: AsiaCrypt '94 will be held in Wollongong, NSW, Australia from 28 November to 1 December, 1994. Jennifer Seberry is the General Chair and Josef Pieprzyk is the Program Chair. AsiaCrypt '96 will be held in Korea in November, 1996. General Chair is Man Young Rhee and Program Chair is Sang Jae Moon.

Peter Landrock reported that he had received a request and responded favorably for 1994 Leuven Algorithms Workshop to be held in December , 1994 to be "in cooperation with IACR".

(IACR BOD meeting, Crypto '94 continued)

It was decided that an ad hoc committee be set up to investigate the impact of making AsiaCrypt "sponsored by IACR" instead of "in cooperation with IACR". The ad hoc committee members are: Ingemar Ingemarsson, Hideki Imai and Tom Berson. A report from this committee should be prepared for the BOD meeting at EC '95.

BYLAWS: The revised IACR Bylaws were approved by the membership.

JOURNAL OF CRYPTOLOGY REPORT: Gilles Brassard, the Editor of the Journal, reported that all is going well with the Journal. However submission rate is down and it would be premature at the moment to increase to four 64 page issues per year. Gilles would like for the associate editors to solicit good papers to be submitted to the Journal.

Gilles is going on sabbatical and asks that the IACR pay to ship his files. This was discussed by the BOD and approved. Gilles to submit budget to Kevin. McCurley.

Kevin McCurley made the motion for Gilles Brassard to continue as Editor of the Journal for two more years. This was seconded by Scott Vanstone. All were in favor.

FINANCIAL REPORT: Kevin McCurley reported that he has completed the IACR 1993 tax return. If any one is interested in seeing it, please contact Kevin. Kevin also a recommended that membership fees not be increased this year.

MEMBERSHIP SECRETARY'S REPORT: Andy Clark, the Membership's Secretary, reported that he with the help of Jimmy Upton and Michele Treolo have merged all the previous databases into one. Andy has applied for registration of the IACR database with the UK Data Protection Registrar.

Andy has yet to receive a list of attendees from EC '94 (Peter will remind William Wolfowicz).

Anyone needing to contact the Membership Secretary can do so at the following address: I.A.C.R., P. O. Box 743, Brighton, East Sussex, BN1 5 HS, U.K. Email address is iacrmem@crypto.demon.co.uk

CONFERENCE PROCEEDINGS: Tom Berson made a motion to accept the new arrangements proposed by Springer Verlag for publishing the proceedings for the IACR conferences. Gilles Brassard seconded the motion. There was one abstention. All others in favor. Motion passed.

COMMITTEE REPORTS: General Chair Guidelines Committee: Because of Jennifer Seberry's recent illness, it was decided to have other volunteers to work on revising the General Chair Guidelines. Paul Van Oorschot and Andy Clark volunteered. A report should be available at the BOD meeting at EC '95.

Program Chair Guidelines Committee: Yvo Desmedt, Program Chair for C '94, joined the meeting to discuss the Program Chair Guidelines. Yvo stressed that the Guidelines should allow the Chair flexibility. The committee consisting of Peter Landrock, Ingemar Ingemarsson, Rainer Rueppel and Sherry Shannon will meet during the week to discuss further. Draft revised Guidelines should be available within one month and sent out for vote to all the BOD members by the end of December, 1994.

Honors Committee: Committee members were Whit Diffie, Rainer Rueppel and Bob Blakley. The Committee recommended the establishment of an IACR Distinguished Lecturer (DL) . Rainer will provide at EC '95 the guidelines/criteria for selection. The DL will present an invited talk to Crypto. The BOD decided to have Scott Vanstone, Kevin McCurley and Jean-Jacques Quisquater to select the next Distinguished Lecturer based on the following criteria: outstanding new work, long standing good work and contributions to the community. Gus Simmons is honored as the first Distinguished Lecturer and is presenting an invited talk to C '94.

1994 ELECTION: The 1994 election will be for three director positions presently held by Paul Van Oorschot, Tom Berson and Hideki Imai. The 1994 Election Nomination Committee members are: Sherry Shannon (the returning officer), Gord Agnew and Jean-Jacques Quisquater.

(IACR BOD meeting, Crypto '94 continued)

RESIDENT AGENT: Because of the dissatisfaction with the resident agent, a motion was made by Tom Berson to have Kevin McCurley find a new resident agent for the IACR. The motion was seconded by Gord Agnew. All were in favor.

OTHER BUSINESS: It was decided to have Jimmy Upton and Kevin McCurley to check into registering "iacr.org". It was also decided to have Kevin McCurley find out how to allow the use of credit cards for the IACR conferences.

There was a discussion of late fees and whether late fees discouraged the attendance of students to the IACR conferences. The General Chair Guidelines do not address late fees, however for the last three years late fees have been in place for Crypto and Eurocrypt.

PREPARATION FOR GENERAL ASSEMBLY: Peter Landrock mentioned what reports he wanted presented at the General Assembly.

Meeting adjourned.

GENERAL ASSEMBLY OF THE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH AT CRYPTO '94

Peter Landrock, the president of IACR, called the General Assembly to order at approximately 4:30 p.m. on Wednesday, August 24, 1994. Peter introduced the IACR officers and directors.

CRYPTO '94: Peter presented certificates of appreciation to Jimmy Upton, General Chair of C '94, and Yvo Desmedt, Program Chair of C '94.

MEMBERSHIP: Peter reported that there are 458 IACR members

ELECTION: Gord Agnew spoke about the upcoming 1994 election and the balloting procedure.

IACR NEWSLETTER: Gord Agnew, Editor of the IACR Newsletter, solicited input to the Newsletter.

JOURNAL OF CRYPTOLOGY: Gilles Brassard gave his report.

BYLAWS: It was reported that the revised Bylaws were approved by the membership.

MEMBERSHIP SECRETARY: Andy Clark gave his report.

QUESTIONNAIRE: Peter mentioned the questionnaire and that the purpose was to gain input from the members on issues that have been brought up in the past by members.

CONFERENCES: Peter gave an overview of the upcoming conferences (see BOD minutes).

OTHER BUSINESS: Peter mentioned Michael Baum's new book on legal aspects of electronic authentication, etc. etc.; Ross Anderson spoke about the *Security Review* that he edits; John Gilmore asked about the IACR Financial Report and Peter responded that the report is published in the Newsletter. Someone asked about an electronic announcements of all IACR conferences, call for papers, etc. Peter agreed to have the BOD look into this.

Meeting adjourned.

Respectfully submitted,

Sherry E. Shannon

Sherry E. Shannon
IACR Secretary