

MINUTES
IACR Board of Directors Meeting
Eurocrypt 89, Houthalen, Belgium
April 10-13, 1989

Present: T Berson
G Agnew
D Chaum
P Landrock
I Ingemarsson
N Cott
J Seberry
J Vandewalle
J Gordon
T Beth
J Massey
T Matsumoto
E Brickell
J Quisquater
A Clark
L Nilsen
W Diffie
R Rueppel

The meeting was called to order at 12:30 on 11 April 89.

1. Apologies for absence
There were no apologies for absence.
2. Minutes of the last meeting
The minutes of the last meeting were accepted as a correct record.
3. Resignation of Secretary/Treasurer
The Board of Directors accepted the resignation of Wyn Price with regrets. Personal reasons had made it impossible for W Price to continue serving the IACR as S/T. The Board of Directors expressed its gratitude for the time and effort that Wyn Price had dedicated to the IACR.
4. Appointment of substitute Secretary/Treasurer
The proposal to appoint R Rueppel as substitute Secretary/Treasurer was accepted unanimously.
5. Resignation of certain Directors
The resignations of H Beker and S Kent (whose written confirmation was received after Eurocrypt 89) were accepted with regret. The BoD expressed its gratitude for their service.
6. Appointment of new Directors
It was agreed that the appointment of new directors should be delayed until after the bylaws discussion. It was generally felt that a Director ideally should play an active role in the development of the IACR, and that he/she should devote a minimal time to the IACR.

7. Financial Report (T Berson)

The Financial Report indicated that IACR was in sound financial position. Yet there was a discrepancy between the income surplus and the change in assets which made it necessary to delay acceptance of the financial report. The issue of auditing the accounts was discussed. J Seberry suggested that an internal audit might be useful. The general feeling was that if the S/T considered an outside auditing of the accounts to be necessary he was allowed to do so. But there exists no legal requirement for an external auditing.

8. Report of Bylaws Committee (J Massey)

J Massey gave a short account of the history of the IACR Bylaws. In the first issue of the IACR Newsletter the current Bylaws had been proposed but never officially accepted. In 84 a Bylaw revision was attempted under the guidance of D Denning; the revision was never put to vote nor adopted. The same fate happened to the 87 attempt of a second revision under guidance of T Berson. In 88 a committee was appointed (J Massey W Diffie D Kahn) to draft a proposal. The proposal was sent to D Denning and T Berson; both replied with several questions/suggestions. The draft Bylaws prepared under guidance of J Massey were distributed to BoD members. It was agreed that the BoD should have some time to study the Bylaws proposal before entering a discussion.

9. IACR Conference Guidelines

The current version dates from April 86 and was prepared by D Denning and T Berson. A committee (J Massey, G Agnew, H Fredericksen, E Brickell) was appointed in 88 to revise Conference Guidelines. The following questions/suggestions were discussed: (1) The S/T should maintain the document. (2) Until further notice the statement "...in cooperation with the IEEE Committee on Security and Privacy.." will be included in the conference announcements of the IACR; a letter of commitment should be exchanged between the IACR and the IEEE. (3) Mailing point: It was felt appropriate that the initial mailing of conference announcements and the mailing of the Newsletter should be handled centrally. However, a Motion by T Beth was unanimously agreed upon: The Secretary should look into hiring a professional post service that would do the central mailings for the IACR. (4) The confidentiality of mailing labels was discussed with the result that the issue of a Membership Directory was declared to be a new business item. (5) A list of addresses of organizations where the conference announcements should be sent is to be included in the CG's. (6) A list of Journals where the Call for Papers should be published is to be included in the CG's. (7) Every Local Arrangements Committee should have a contingency plan in case many more participants register than expected (see below under Eurocrypt 90).

10. Asiacypt (T Matsumoto)

Asiacypt will be held in Japan (exact location not yet specified) November 11-14, 1991. Prof. Tsujii will be General Chairman.

11. Eurocrypt 90 (P Landrock)

P Landrock reported that planning for Eurocrypt 90 in Aarhus, Denmark, May 21-24, was well under way. But, suprised by the 300 attendees of Eurocrypt 89, he feared that the conference center of choice (Scanticon) would not be able to hold this many participants. A general discussion evolved around the questions: Is there a way to control the size of IACR conferences? Is there a need to change policy? Parallel sessions; tutorial sessions? Workshop vs. Conference? The discussion concluded that this item be entered under New Business. The Program Chairman was still to be elected (C Schnorr and J Massey were possible candidates).

12. Eurocrypt 89 (J Vandewalle, J Quisquater)

J Vandewalle reported that about 300 had come to attend Eurocrypt 89, the largest number

ever; the financial report will be presented at Crypto 89. J Quisquater reported that 82 papers had been submitted of which were accepted 57 (including the poster session). I Ingemarsson expressed concern on the density of the program. D Chaum suggested that blind reviews should be adopted in general. Thanks were expressed to J Vandewalle and J Quisquater for their excellent work.

13. Auscrypt 90 (J Seberry)

It was reported that planning for Auscrypt 90 was well under way. Because of the late mailing of the conference announcements containing the call for papers it was agreed that the deadline for submissions be extended by 1 month until May 31, 89.

14. Proposals for Eurocrypt 91 (L Nilsen, A Clark) L Nilsen presented a proposal for holding Eurocrypt in Norway. A Clark presented two alternatives for holding Eurocrypt in England. In the final vote the University of Sussex was selected as appropriate place. It was felt that this academic environment might create some workshop atmosphere. The final date was not yet fixed; A Clark will be General Chairman and D Davies will be Program Chairman. Thanks go to L Nilsen and his colleagues for preparing the Norwegian proposal.

15. Journal for New Members (T Berson)

Because of the delay in publication of the JoC T Berson put forward the Motion that all attendees of Eurocrypt 89 or Crypto 89 who become new members of the IACR will receive both Vol 2 and Vol 3 of the JoC. The Motion was unanimously agreed upon.

16. Journal of Cryptology (E Brickell)

It was reported that the JoC had found widespread acceptance: 367 libraries had subscribed to the Journal. But unfortunately, due to the slow review and revision process, the JoC will suffer a temporary delay of about 6 months. The next issue (Vol 1/3) will appear end of July. Consequently, Vol 2 will be published in 90 instead of 89. It was asked if one could not simply reassociate Vol 2 with 1990. But since the agreement with Springer specifies that one volume be published per year, it is only to be hoped that soon the JoC will be back in normal publication rhythm.

17. Newsletter (G Agnew)

It was reported that the Newsletter was running thin of submissions, and that the Editor would assign writing tasks if necessary.

18. SmartCard 2000 (D Chaum)

The next SmartCard 2000 Meeting will be held on October 4-6, 89, at a location that still has to be specified.

The meeting closed at 14:15 on April 12 (two business lunches).

Rainer A Rueppel
Secretary/Treasurer
May 19, 1989