BYLAWS OF THE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, INC. (Revised November 1997)

With proposed revisions, September 1998

Article I: Name

The name of this organization is the International Association for Cryptologic Research, Inc., hereinafter referred to as the IACR.

Article II: Purposes

The purposes of the IACR are to advance the theory and practice of cryptology and related fields, and to promote the interests of its members with respect thereto, and to serve the public welfare. To achieve these purposes, the IACR sponsors the **Asiacrypt,** Eurocrypt and Crypto conferences, sponsors or co-sponsors other appropriate meetings or conferences, co-operates with appropriate meetings or conferences sponsored by other groups, publishes a journal and a newsletter, and takes such other actions as its Board of Directors, hereinafter referred to as the Board, deems appropriate.

Article III: Membership

Membership is open to any person subscribing to the purposes of the IACR. A person becomes a member or renew~~ed~~**s** his or her membership either of two ways: 1) upon acceptance by the IACR Membership Secretary of his or her personal membership application form and payment of one year's dues or 2) notification to the IACR Membership Secretary by the General Chairperson of attendance at either **Asiacrypt,** Eurocrypt or Crypto.

As described in Article VII, the form for acquiring or renewing membership is incorporated into the registration form**s** for the **Asiacrypt,** Eurocrypt **and**~~or~~ Crypto conferences. The form also can be obtained from the Membership Secretary.

Membership period as a result of attending a**n Asiacrypt,** Eurocrypt or Crypto conference in year n, begins on January 1 (year n+1) and ends on December 31 (year n+1).

Membership applications (other than as a result **of**~~for~~ attending a**n Asiacrypt,** Eurocrypt or Crypto conference (see above)) for year n are processed from 1 September (year n-1) until 31 August (year n). Individuals applying at any time during the year pay the full membership fee. Membership begins on January 1 of the date year n and expires on December 31 of year n.

There are two categories of personal membership: regular and student. Student members must be enrolled in an institution of learning.

Membership, whether regular or student, entitles the member to receive the Journal of Cryptology and the IACR Newsletter with no additional payment of fees. For those individuals whose membership is accepted after the first issue of the Journal of Cryptology and/or the IACR Newsletter has been mailed, back copies of all publications to which they are entitled will be sent by the Membership Secretary together with the membership confirmation.

A member who engages in an activity inconsistent with the purposes of the IACR may be expelled from the IACR by a three-fourths vote of the full Board. The member under investigation has the right to examine the charges against him or her and to make a statement defending himself or herself before the vote. The proceedings and documentation are confidential, unless the member wishes to make them public. An expelled member may be reinstated, at the earliest, one year after his or her expulsion

by a majority vote of the Board.

Changes in the amount of dues in the next calendar year for any class of membership are proposed by the Board to the Assembly for approval at the **Asiacrypt, Eurocrypt, or** Crypto conference.

Article IV: Officers

The Officers of the IACR are the President, the Vice President, the Secretary, and the Treasurer. One person may hold only one office, and only a regular member may serve as an Officer. The term for all offices is three calendar years. Officers may serve successive terms. The Officers are elected by the members by secret ballot.

The President, in addition to his or her other duties as described elsewhere herein, is responsible, under the supervision of the Board, for the day-to-day functioning of the IACR. The President represents the IACR in its dealings with other organizations. The President appoints committees as required to assist him or her in discharging these duties. The President publishes an Annual Report to the membership on the past year's activity of the IACR in the first issue of the IACR Newsletter in each calendar year.

The Vice President performs such duties as the President or the Board may assign. The Vice President acts for the President in the President's absence. The Vice President becomes Acting President until the next regular election upon the death, incapacity, resignation, or expulsion of the President.

The Secretary, in addition to his or her other duties as described elsewhere herein, is responsible for maintaining the minutes of the Board meetings, the guidelines and the Bylaws of the IACR and for co-ordinating with the Membership Secretary the timely mailing of announcements.

The Treasurer is responsible for the receipt and payment of funds on behalf of the IACR and for the maintenance of proper financial records and documents. The Treasurer recommends to the Board ~~at its session during the Crypto conference~~ any changes in the amount of dues to be paid by the membership in the following year. The Treasurer publishes the annual Financial Report of the IACR in the first issue of the IACR Newsletter in each calendar year.

The Board at its discretion may establish a secretariat with paid personnel to assist the Officers in activities as the Board may direct.

Article V: Board of Directors

The Board (in any calendar year) consists of the Officers, the General Chairpersons of the **Asiacrypt,** Eurocrypt and Crypto conferences for that year and the following year, the Editor of the Journal of Cryptology, the Editor of the IACR Newsletter, the Membership Secretary, and nine elected Directors. The term of office of the nine elected Directors is three calendar years with three terms expiring each year. Directors are elected by secret ballot of the members. Elected Directors may be re-elected.

The General Chairperson for **each**~~all~~ conference~~s~~ sponsored by the IACR is appointed by the Board and serves for one calendar year. These appointments are made two years in advance. The General Chairperson has full responsibility for arranging all aspects of the conference except for the technical program and may appoint whomever he or she wishes to assist in the execution of these duties.

The Editor of the Journal of Cryptology is appointed by the Board for a term of a maximum of three years and can be reappointed. He or she is responsible, under the supervision of the Board, for the editorial policy of the Journal. The Editor of the Journal appoints, with the advice and consent of the

Board, such Associate Editors as are required to assist him or her in the discharge of his or her duties. Associate Editors serve at the pleasure of the Editor.

The Editor of the Newsletter is appointed by the Board for a term of a maximum of three years and can be reappointed. He or she is responsible, under the supervision of the Board, for editorial policy, production and distribution of the Newsletter.

The Membership Secretary is appointed by the Board of Directors for a term of a maximum of three years and can be reappointed. The Membership Secretary is responsible for maintaining the records of the members which include the mailing list.

The Board further appoints the Program Chairperson for ~~all~~**each** conference~~s~~ sponsored by the IACR. The Program Chairperson is not a member of the Board. These appointments are made two years in advance. The Program Chairperson appoints a program committee to assist him or her in ensuring that the program meets a high scientific standard.

The Board, under the supervision of the Assembly, manages, controls and directs the affairs, funds, and property of the IACR. The Board meets **at least once** ~~twice~~ annually~~,~~**. These meetings are** at **varying locations among** the **Asiacrypt,**Eurocrypt and Crypto conferences, each time prior to the respective Assembly. The Board may also transact ~~urgent~~ business ~~that arises~~ between these semiannual sessions by post, telephone, and/or electronic mail.

Meetings of the Board are presided over by the President of the IACR, or, in case of the President's absence, by the Vice President, or, in case of both their absences, by the Secretary. Minutes of Board meetings and of the Assembly are kept by the Secretary or, in case of the Secretary's absence, by a member of the Board designated by the Secretary as his or her representative. These minutes, after mail approval and/or correction by the Board, are published in the IACR Newsletter as soon as practical after the meeting.

A majority of the Board **(including proxies)** constitutes a quorum at the ~~semiannual~~ meetings. Decisions are made by a majority vote of the Directors present (including proxies) or by a majority vote of the full Board for actions taken outside of the ~~semiannual~~ meeting**s**. Each member of the Board may cast only a single vote no matter how many roles place him or her on the Board. The President votes only to break ties in the voting by the other Directors.

Article VI: Publications

The IACR publishes the Journal of Cryptology and the IACR Newsletter, hereinafter referred to as the Journal and the Newsletter, respectively. The Journal publishes carefully reviewed papers of an archival nature. The Newsletter publishes items of current interest such as notices of meetings or conferences related to cryptography, calls for papers, cryptographic news, and the like.

Article VII: Meetings and Conferences

The IACR sponsors ~~two~~ regular annual conferences, **the Asiacrypt conference,** the Eurocrypt conference, ~~which is held in the spring in Europe,~~ and the Crypto conference~~, which is held in late summer in North America~~. The IACR may sponsor, or co-sponsor, additional meetings or conferences as the Board deems appropriate. The IACR may co-operate, without financial responsibility, in other worthy meetings or conferences as deemed appropriate by the President and approved by the Board.

The registration form of the **Asiacrypt,** Eurocrypt and Crypto conferences also serves as the usual form for renewing of regular or student membership in the IACR. The fee for participating in these conferences includes the annual dues for the next year; this fee is paid in full even by those who do not desire to become IACR members. The option not to become or remain an IACR member must be available on the registration form, which must clearly explain that the fee is the same whether or not one desires membership. Registrants must indicate in writing the desired option.

Article VIII: Assembly

Assemblies of the membership take place **three times** annually, at the Eurocrypt**, Asiacrypt, and** ~~conference and at the~~ Crypto conference. Each Assembly is presided over by the President of the IACR or, in case of the President's absence, by the Vice President, or, in case of both their absences, by the Secretary. The Assembly is open to all members of the IACR. Twenty-five members constitute a quorum for business at an Assembly.

The President or his or her representative places before the Assembly those decisions made by the Board, since the most recent Assembly, that were designated by the Board as major decisions requiring confirmation by the Assembly. The Assembly either accepts these decisions or rejects them by majority vote of the members present. Motions may also be proposed from the floor by any member and, if seconded by another member, adopted by majority vote of the members present.

When the President judges that an action taken by the Assembly does not reflect the position of a majority of the members of the IACR, the President may place the question before the entire membership in a written ballot. If 10 percent of the members petition the Board for a referendum on an issue, the Board directs the Secretary to place the question before the entire membership in a written ballot within six weeks. The Secretary, in co-ordination with the Membership Secretary, mails ballots within six weeks of the President's decision or of receipt of a petition. Ballots indicate the date of counting, which is at least six weeks from the mailing date. No ballots returned by members will be counted if received after the designated date of counting.

Article IX: Elections

~~At its session during the Eurocrypt conference~~**Each year not later than May 31**, the Board appoints three or more of its members as a committee to nominate candidates for the elected regular member positions of the Board and, every three years, to nominate candidates for the posts of President, Vice President, Secretary and Treasurer. This committee (referred to as the Nomination/Election Committee) is also responsible for the carrying out of the election and selects its own chairperson and returning officer. ~~The chairperson presents the list of positions for the upcoming election to the Assembly at the next Crypto conference and opens up the nominations~~. **The committee opens up the nominations no later than June 15. The list of positions for the following election is presented at every Assembly.** Any IACR member can nominate another regular member and all nominations must be made in writing to the chairperson. The ballot with the names of all nominees for each office thereon is mailed by the Nomination/Election Committee not later than October 1 of each year to all members with instructions that the ballot, in order to be counted, must be received at a designated address by November 15. The returning officer, together with two independent persons appointed by him or her for this purpose, counts the ballots as soon as practicable after November 15 and reports the results to the candidates as well as to the Board. Results of the election are to be published in the next IACR Newsletter. All mail elections are decided by a plurality of ballots cast. In the event of a tie, the Board votes by mail ballot until the tie is broken.

Any premature vacancy in an elected or appointed office is filled for the remainder of the regular term by an appointee chosen by the President and then approved, as soon as possible, by the Board.

Any member of the Board who engages in an activity inconsistent with the purposes of the IACR may be removed from office upon three-fourths vote of the full Board. The person under investigation has the right to examine the charges against him or her and to make a statement defending himself or herself before the vote. The proceedings and documentation are confidential, unless the person under investigation wishes to make them public.

Article X: Guidelines

The Board may establish Guidelines as deemed necessary to aid in the activities of the IACR. There will be Guidelines for the General Chairperson and Program Chairperson of the conferences, the IACR Elections, Membership Secretary and others as deemed necessary by the Board. The President, when deemed necessary by the Board, will appoint an ad hoc committee to review the individual Guidelines and update as necessary for presentation to the Board for approval. The Secretary will be responsible for keeping the Guidelines.

Article XI: Amendments

Amendments to these Bylaws may be proposed by majority vote of the Board or at an Assembly by a two-thirds vote of the members present. A proposed amendment becomes effective upon subsequent ratification by a majority of the ballots cast in a mail referendum to the members.