

BYLAWS OF THE INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, INC.

Approved 22 December 2008

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 its own conferences (the "IACR Conferences") and workshops (the "IACR Workshops"), sponsors or co-sponsors other appropriate meetings or conferences, co-operates with appropriate meetings or conferences sponsored by other groups, publishes a journal and ~~an electronic communication portal-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.

There are ~~threetwo~~ categories of membership: student, regular, and studentsenior. Student members must be enrolled as a student in an institution of learning.

A person becomes a regular or student member or renews his or her regular or student membership in 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 any one of the IACR Conferences or IACR Workshops.

A member can become a senior member in any calendar year following the year in which he or she has reached the age of 65, provided that he or she has been a regular or student member for at least twenty years (not necessarily consecutive). Members can apply for senior membership by submitting a request in writing to the IACR Membership Secretary. Senior membership holds for the lifetime of the member and does not need to be renewed. The IACR intends not to charge membership dues for senior members in recognition of their demonstrated long-time membership; the procedures of Article XIV for setting the membership dues apply

All members have electronic access to the Journal of Cryptology and to the publications from recent IACR Conferences and Workshops. A print subscription of the Journal of Cryptology is

~~available at an extra cost. 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.~~

Membership period as a result of attending an IACR Conference or IACR Workshop is for the calendar year following the workshop. The calendar year begins on January 1 and ends on December 31.

Membership applications (other than as a result of attending an IACR Conference or IACR Workshop) processed on or before August 31 in any given year will apply to that calendar year. Membership applications processed from September 1 onward will apply to the following calendar year. Regardless of the time of application and becoming a member, the membership fee for the full calendar year needs to be paid. ~~Individuals applying at any time during the year pay the full membership fee.~~

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 members elect the Officers 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 quarter 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 publishes the annual Financial Report of the IACR in the first quarter 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 consists of the Officers, the nine Elected Directors and the Appointed Directors.

The term of office of the nine Elected Directors is three calendar years with three terms expiring each year. Elected Directors are elected by secret ballot of the members. Elected Directors may be re-elected.

The Appointed Directors (in any calendar year) are the General Chairpersons of the IACR Conferences for that year and the following year, the Editor of the Journal of Cryptology, the ~~Communications Secretary~~~~Editor of the IACR Newsletter~~, and the Membership Secretary. The Board at its discretion may appoint a limited number of additional non-voting members.

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 annually. These meetings are at varying locations among the IACR Conferences, each time prior to the respective Assembly. The Board may also transact business between these 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 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 meetings. Decisions are made by a majority vote of the Directors present (including proxies) at meetings or by a majority vote of all members of the Board for actions taken outside of the meetings. 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: Elections

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 Director 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 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 member for election as a Director and any other regular member for election as an Officer. All nominations must be made in writing to the chairperson. The Nomination/Election Committee transmits the ballot with the names of all nominees for each office thereon not later than October 15 of each year to all members with instructions for returning the ballots. These instructions must include the statement that in order to be tallying procedure, which must be

verified by at least two independent persons. The returning officer reports the results to the candidates as well as to the Board as soon as practicable after November 15. Results of the election are to be published ~~in the next IACR Newsletter~~. All elections are decided by a plurality of ballots cast. In the event of a tie, the Board votes until the tie is broken. Elections and referenda may be conducted by post or by electronic means at the discretion of the Board. Substantial change to the voting system requires prior approval of the membership, except that the paper-ballot system used by the Association from its inception through 2008 may be used at any time without such approval. Such approval can be obtained either by majority vote at any Assembly or by majority of the ballots cast in a referendum to the members.

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.

Article VII: General Chairperson

The Board appoints the General Chairperson for each IACR Conference. These appointments are normally 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.

Article VIII: Program Chairperson

The Officers and Elected Directors appoint the Program Chairperson for each IACR Conference. These appointments are normally 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.

Article IX: Editor of the Journal of Cryptology

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.

Article X: ~~Editor of the Newsletter~~ Communications Secretary

The Communications Secretary ~~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, content management, and publishing in the electronic communication portal. ~~production and distribution of the Newsletter~~.

Article XI: Membership Secretary

The Membership Secretary is appointed by the Board 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.

Article XII: Publications

The IACR publishes the Journal of Cryptology and the Communications Portal-IACR Newsletter, hereinafter referred to as the Journal and the Newsletter-Portal, respectively. The Journal publishes carefully reviewed papers of an archival nature. The Newsletter-Portal publishes items of current interest such as notices of meetings or conferences related to cryptography, calls for papers, cryptographic news, and the like. The Communication Portal may be implemented by a website or other forms of electronic distribution.

Article XIII: Meetings and Conferences

The IACR takes full financial responsibility for the IACR Conferences and IACR Workshops. 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.

Article XIV: Membership Dues

The registration form of the IACR Conferences and IACR Workshops also serves as the usual form for renewing of membership in the IACR. The fee for participating in these events includes the annual dues for the next year; even those who do not desire to become IACR members pay this fee in full. 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.

The Treasurer recommends to the Board any changes in the amount of dues to be paid by the membership in the following year. Changes in the amount of dues in the next calendar year for any class of membership are proposed by the Board to an Assembly for approval.

Article XV: Assembly

Assemblies of the membership take place annually, at each of the IACR Conferences. 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, sends 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 sending date. No ballots returned by members will be counted if received after the designated date of counting.

Article XVI: Disciplinary Matters

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.

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.

Article XVII: 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 XVIII: 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 referendum to the members.