Bylaws of the International Association For Cryptologic Research

~~Approved 16 November 2019~~ Version for approval, October 2025 *

(**Note:** Green annotations such as this one are not part of the proposed revised Bylaws. They provide additional explanations in the context of the vote to approve the Bylaws modification.

Text in blue such as this example is new text, proposed to be added to the Bylaws. Text in red such as ~~this example~~ is text from the current Bylaws, proposed to be removed.)

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, sponsors or co-sponsors other appropriate meetings, workshops, or conferences, co-operates with appropriate meetings, workshops, or conferences sponsored by other groups, publishes ~~a journal (the Journal of Cryptology)~~academic journals, maintains an electronic communication portal, and takes such other actions as its Board of Directors, hereinafter referred to as the Board, deems appropriate.

The Journals published by the IACR include the Journal of Cryptology, the IACR Communications in Cryptology, and Area Journals[1]. (**Note:** This addition acknowledges the growing list of IACR publications. It mirrors the following sentence listing Conferences.)

The Conferences sponsored by the IACR consist of General Conferences,[2] Area Conferences,[3] and Symposia.[4]

---

*The most recent version of this document can be obtained from `http://www.iacr.org/docs/`

[1] As of 2025 the Area Journals are the IACR Transactions on Symmetric Cryptology (ToSC) and the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES).

[2] As of ~~2016~~ 2025 the General Conferences are the annual Asiacrypt, Crypto, and Eurocrypt conferences.

[3] As of ~~2016~~ 2025 the Area Conferences are the annual CHES (Cryptographic Hardware and Embedded Systems), FSE (Fast Software Encryption), PKC (Public Key Cryptography), and TCC (Theory of Cryptograhy Conference) conferences.

[4] As of ~~2019~~2025, the Real World Cryptography symposium.

Article III: Membership

Membership is open to any person subscribing to the purposes of the IACR.

There are three categories of membership: student, regular, and senior. 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~~ their regular or student membership in either of two ways: 1) upon acceptance by the IACR Membership Secretary of ~~his or her~~ their 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~~ registration at any one of the IACR Conferences.

(**Note:** The following paragraph is a reordered and clarified version of the last two paragraphs of the article in the current Bylaws.)

Membership period is for a full calendar year. The calendar year begins on January 1 and ends on December 31. Membership granted as a result of registration to an IACR Conference is for the calendar year following the event. Other membership applications processed on or before September 30 in any given year will apply to that calendar year. Membership applications processed from October 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.

A member can become a senior member in any calendar year following the year in which ~~he or she has~~ they have reached the age of 65, provided that ~~he or she has~~ they have 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~~ does not charge membership dues for senior members in recognition of their demonstrated long-time membership; the procedures of Article ~~XIV~~ XVI for setting the membership dues apply.

All members have electronic access to ~~the Journal of Cryptology and to the publications from recent IACR Conferences. A print subscription of the Journal of Cryptology is available at an extra cost.~~ all IACR publications. (**Note:** All IACR publications are accessible to Members.)

(**Note:** The following two paragraphs have been moved (with small modifications) two paragraphs earlier.)

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

~~Membership applications (other than as a result of attending an IACR Conference) processed on or before September 30 in any given year will apply to that calendar year. Membership applications processed from October 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.~~

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 non-student 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~~ their 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~~ them 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 of 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~~ their 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~~ Communications 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 of 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 General Conferences for that year and the following year, the Editor of the Journal of Cryptology, an Editor of the IACR Communications in Cryptology, the IT Manager, the Communications Secretary, and the Membership Secretary. (**Note:** With this modification, an Editor of the IACR Communications in Cryptology will be an Appointed Director of the Board of Directors. This change mirrors the situation of the Editor of the Journal of Cryptology.) In cases where Co-Editors or Co-Chairpersons share a responsibility, they may, subject to approval by the Board, decide which of them joins the Board. The Board at its discretion may appoint ~~a limited number of~~ additional non-voting members. Any premature vacancy in an 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. (**Note:** In the current version of the Bylaws, this provision on premature vacancy of appointed positions is written in *Article VI: Elections*.)

The Board, under the supervision of the Assembly manages, controls, and directs the affairs, funds, and property of the IACR. The Board meets in person at least once annually. These meetings take place at varying locations among the IACR General Conferences, each time prior to the respective Assembly. The Board may also meet via teleconference or other electronic means or transact business between meetings by post, telephone, and/or electronic means.

Meetings of the Board are presided over by the President, 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~~ their representative. These minutes, after approval and/or correction by the Board, are published as soon as practical after the meeting.

More than 2/3 of the members of the Board (including proxies) constitutes a quorum at the meetings. Decisions are made by a majority vote (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~~ them on the Board. The President votes only to break ties in the voting among the members of the Board.

The Board may establish Steering Committees to aid with the organization of repeatedly-occurring Conferences. A member of each such Steering Committee serves as a representative to the Board and participates as an observer in its meetings.[5]

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~~ administer the nomination process 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. (**Note:** This modification reflects the fact that the Election Committee does not itself nominate candidates: it only administers the process.) 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 in the year of the election can nominate another member for election as a Director and any other non-student 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 31 of each year to all members with instructions for returning the ballots. These instructions must include a cutoff date until when a ballot must be received for counting; the period from the sending of ballots to the cutoff date must be at least 30 days. The returning officer oversees the 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 30. Results of the election are to be published. 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.

[5] As of ~~2019~~ 2025 there are Steering Committees for Asiacrypt, RWC and for all Area Conferences.

Article VII: General Chairperson

A General Chairperson ~~is~~ (or two General Co-Chairpersons) is (or are) appointed for each IACR Conference. (**Note:** This modification reflects the fact that with the increasing scale of our events, there are often two General Co-Chairpersons.) 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~~ they wish to assist in the execution of these duties.

For IACR General Conferences the appointment is made by the Board, normally at least two years in advance. For IACR Area Conferences the respective Steering Committee selects a General Chairperson and proposes this to the Board; the Board will approve the proposal or ask for revisions.

Article VIII: Program Chairperson

A Program Chairperson ~~is~~ (or two Program Co-Chairpersons) is (or are) appointed for each IACR Conference. (**Note:** Like for General Co-Chairpersons, there are often two Program Co-Chairpersons for IACR Conferences.) The Program Chairperson appoints a program committee to assist ~~him or her~~ them in ensuring that the program meets a high scientific standard.

For IACR General Conferences the appointment is made by the Officers and Elected Directors in the Board, normally at least two years in advance. For IACR Area Conferences the respective Steering Committee selects a Program Chairperson and proposes this to the Board; the Board will approve the proposal or ask for revisions.

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~~ They are 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~~ them in the discharge of ~~his or her~~ their duties. (**Note:** The Editor does not consult with the Board for the selection of Associate Editors (the Editorial Board). The supervisory role of the Board is the object of the previous sentence.) Associate Editors serve at the pleasure of the Editor.

Article X: Co-Editors of the IACR Communications in Cryptology

(**Note:** This new article formalises the appointment and role of the Co-Editors of the IACR Communications in Cryptology. It is similar to the corresponding article for the Journal of Cryptology, Article IX.)

The two Co-Editors of the IACR Communications in Cryptology are each appointed by the Board for a two-year term and may be reappointed. Appointments are staggered, with one editor appointed each year.

The Co-Editors are responsible, under the supervision of the Board, for the editorial policy of the IACR Communications in Cryptology. The Co-Editors appoint such Associate Editors as are required to assist them in the discharge of their duties. Associate Editors serve at the pleasure of the Co-Editors.

Article XI: IT Manager

(**Note:** This new article formalises the appointment and role of the IT manager, a new Appointed Director responsible for the IT infrastructure of the IACR.)

The IT Manager is appointed by the Board for a term of a maximum of three years and can be reappointed. They are responsible, under the supervision of the Board, for the IT infrastructure of the association, its effective operation, security, and maintenance. The IT Manager oversees the work of the IT staff and volunteers, advises the Board on IT strategies, and coordinates technology-related tasks as directed by the Board.

Article XII: Communications Secretary

The Communications Secretary is appointed by the Board for a term of a maximum of three years and can be reappointed. ~~He or she is~~ They are responsible, under the supervision of the Board, for editorial policy, content management, and publishing in the electronic communication portal.

Article XIII: 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 ~~.~~ and of conference participants. For this, the Membership Secretary will liaise with the President, the Treasurer, and the General Chairpersons. (**Note:** This addition provides a more accurate description of the mission of the Membership Secretary.)

Article XIV: Publications

The IACR publishes the Journal of Cryptology ~~and the Communications Portal, hereinafter referred to as the Journal and the Portal, respectively.~~, the IACR Communications in Cryptology, and Area Journals (hereinafter referred to as the Journals), and the Communications Portal (hereinafter referred to as the Portal). The Journals publish carefully reviewed papers of an archival nature. The 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 XV: Meetings and Conferences

The IACR takes full financial responsibility for the IACR Conferences. The IACR may sponsor, or co-sponsor, additional meetings, workshops, or conferences as the Board deems appropriate. The IACR may co-operate, without financial responsibility, in other worthy meetings, workshops, or conferences as deemed appropriate by the President and approved by the Board.

Article XVI: Membership Dues

The registration form of the IACR Conferences also serves as ~~the usual form for~~ a form for application or 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.

For other membership applications (i.e., not resulting from conference registration), the membership dues are processed by the Membership Secretary.

The Treasurer recommends to the Board any changes in the amount of dues ~~to be paid by the membership in the following year~~for the membership period after the next calendar year (i.e., attached to IACR Conference registrations of the next calendar year, or for other membership applications sent from October 1 of the next calendar year). Changes in the amount of dues ~~in~~ after the next calendar year for any class of membership are proposed by the Board to an Assembly for approval. (**Note:** The modification of this paragraph is meant to clarify and simplify the rules for changing the amount of dues. Previously, the timeline for applying changes was based on the year in which the dues were paid rather than the membership year being applied for.)

Article XVII: Assembly

Assemblies of the membership take place annually, at each of the IACR General 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~~. In case of the President's absence, the Assembly is presided over by another Board Member appointed by the President. (**Note:** This modification aims at simplifying the selection of a Board Member to preside over an Assembly in case of the President's absence.) 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~~ their 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 XVIII: 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~~ them and to make a statement defending ~~himself or herself~~ themself before the vote. The proceedings and documentation are confidential, unless the person under investigation wishes to make them public.

A member of the IACR 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~~ them and to make a statement defending ~~himself or herself~~ themself 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~~ their expulsion by a majority vote of the Board.

Article XIX: 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, for Steering Committees of Conferences, for Elections, 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 XX: 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.