IACR Guidelines for Program Chairs

March 2020*

Dear Program Chair(s),

The purpose of this document is to help you run a successful conference program. For the most part it consists of guidelines that are not rigid rules but rather a description of what worked well for past Program Chairs. This document is not complete; there are many issues not addressed here that you will have to think about. Use your own best judgment and feel free to seek out the advice of the members of the IACR Board of Directors ("the Board"), the conference Steering Committee, preceding Program Chairs, and experienced members of the community.

This document also contains a number of rules that represent decisions taken by the Board or by the IACR membership. You are expected to follow these rules: they can be recognized by the imperative "must." Section 1 explains the motivation behind having rules and the division of responsibility between you, the Board, and the General Chair.

Agreeing to be Program Chair or Program Co-Chair of an IACR-sponsored event implies that you will accept these rules and follow the guidelines. If you feel that you are unable or unwilling to do so, or if you desire modifications be made from these guidelines, please contact the Board or the Steering Committee beforehand. Failure to do so may result in someone else being invited to become Program Chair in your place. You are appointed well in advance of the event taking place. In rare cases, these guidelines may be changed by the Board or by the membership, and if this happens, you are expected to cooperate with the Board for the benefit of the IACR.

Your first contact is the *PC Liaison Officer* of the IACR (currently Bart Preneel, `bart dot preneel @ esat dot kuleuven dot be`); please contact him as soon as possible to get advice and insight from previous events, and send feedback and suggestions for improvements of this document to him.

This document is intended for the Program Chairs of the three IACR General Conferences (Asiacrypt, Crypto, and Eurocrypt) and IACR Area Conferences (CHES, FSE, PKC, and TCC). Appendix E contains specific information for CHES and FSE that are Conference/Journal Hybrids. In this document, an *Event* or *Conference* refers collectively to an IACR General Conference or Area Conference. From 2009 onward the IACR General Conferences have used a *rolling co-chair model* and in 2020 this was changed to a *parallel co-chair model*. The Area Conferences are using several models. Section 2 explains your role as a Program Co-Chair.

Above all, the Board hopes that you find your job rewarding.

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

Contributors to this document: Scott Vanstone and Sherry Shannon (1991, 1995), Ueli Maurer (1999, 2001), Lars R. Knudsen (2002, 2003, 2004), Arjen K. Lenstra (2006, 2007, 2008), Josh Benaloh (2010), Christian Cachin (2011–2015, 2019), Nigel Smart (2014–2015), Steven Galbraith (2020), Bart Preneel (2007, 2019, 2020).

Contents

1 Motivation

You as the Program Chair, the Board, and the General Chair have different responsibilities regarding the organization of IACR events.

According to the IACR Bylaws, the Board "manages, controls, and directs the affairs (...) of the IACR" and is therefore responsible to the IACR membership. In this role, the Board is ultimately the place where legally the responsibility lies for the operations of the IACR and for IACR events. The Board sponsors the conference (through taking financial responsibility), maintains contracts with publishers, looks after issues related to copyright, archiving of papers, selection of venues, and so on.

The Board guards the interests of the IACR members. As the field grows, the Board ensures continuity over the years; when the environment changes the Board also responds to changes in the interests of the IACR. Thus, the Board defines the most important aspects of an event (length, format, publication venue, etc.) as described in this document. Many of these matters require liaison with various external entities (publishers, for example) and imply contractual obligations on or by the IACR. The Board also maintains infrastructure whose goal is to help the organization of events (reviewing software, membership database, the Cryptology ePrint Archive, CryptoDB etc).

Each IACR Area Conference has a Steering Committee that may provide complementary guidelines and rules. As Program Chair of an IACR Area Conference, your first point of contact is the Steering Committee Chair, who can coordinate discussions inside the Steering Committee and with the IACR Board; you should contact the PC Liaison Officer for policy-related issues such as the update of these guidelines.

As Program Chair, you have full responsibility for implementing a fair submission and reviewing process based on the highest scientific and ethical standards. Decisions about the scientific program, e.g., which papers and talks to include are independently taken by you and your Program Committee. The Board (or the Steering Committee) does not interfere with the selection of papers as long as these guidelines are followed. However, the Board (and/or the Steering Committee) may give advice which you may find useful on the selection of the committee, as it provides the collective memory of the IACR. Note: the Program Chair may be involved in the selection of affiliated workshops, but this has typically been the responsibility of the General Chair.

The General Chair is responsible for all organizational matters relating to a Conference except for the scientific content. The General Chair is also responsible for the selection of the affiliated workshops, perhaps assisted by a Workshop Chair. The Board delegates the financial management and local organization of an event to the General Chair. The obligations of a General Chair in this regard are outlined in the Guidelines for General Chairs.

2 Program Co-Chairs

From 2020/2021 onwards, IACR uses a *parallel co-chair model* for its General Conferences. This means that two people are appointed as *Program Co-Chairs for each new edition of a conference*. Program Co-Chairs appointed for a given edition of a Conference automatically become *ex officio* members of the program committee of the preceding edition of the same Conference. Note: CHES and TCC follow the parallel co-chair model while FSE has adopted the *rolling co-chair model*. PKC uses the single chair model and sometimes the parallel co-

chair model. More details for the Conference/Journal Hybrids CHES and FSE are provided in Appendix E.

Wherever this document refers to the Program Chair of a Conference in the parallel or rolling co-chair model, it means both Program Co-Chairs.

The Program Co-Chairs of a Conference are both equally responsible for the event. They should agree on a process and working mode between them that suits them. They should bear a comparable share of the workload. The Program Co-Chairs may also consult with the PC Liaison Officer, with the Board of Directors or with the Steering Committee.

The names of the Program Co-Chairs must always appear together in all publications regarding the event, such as in the conference proceedings or on the conference website.

The procedures for selecting Program Chairs are described in Section 5.

3 Timetable

The following timetable lists the key tasks and when they should approximately be completed. All times are in months from time T of your event.

Appendix C contains a more detailed timetable. For the Conference/Journal Hybrids, an adapted timetable is provided in Appendix E.

$T - 18$ Inform yourself about your job, get in touch with your Program Co-Chair (if applicable), and start planning (see Section 4). Contact the PC Liaison Officer for information.

$T - 12$ Select the Program Committee (see Section 5). Run your proposed PC past the PC Liaison Officer and/or the Steering Committee Chair for feedback. Contact Springer about the publication of the proceedings (see Section 11), and get acquainted with reviewing software (see Section 6).

$T - 11$ Write the Call for Papers and put it on the event website (see Section 7).

$T - \{10, 9\}$ Start discussing with your committee issues such as their topics of interest for reviewing, invited speaker(s), and whether or not to have a physical Program Committee meeting. Make sure the submission server is up and running. Finalize budget negotiations with the General Chair (See Section 13),

$T - 7$ The Program Committee members should be able to use the reviewing software.

$T - 6$ Papers have been submitted, reviewing begins (see Section 8). Make rump session policy available (General Chair, event webpage)

$T - 5$ The discussion phase of the reviewing process.

$T - 4.5$ Send to authors the reviews for their rebuttal. Discussions continue. Make final decisions.

$T - 3.5$ Send to authors the decisions (see Section 9), (cleaned up) reviews, and instructions (see Section 10). Finalize discussion on invited speaker(s), and decide on the best paper award. Notify the General Chair of your decisions.

$T-3$ Appoint session chairs, coordinate the programs with the General Chair, and wrap up the reviewing process.

$T-2$ Authors submit the proceedings versions to you. Assemble the proceedings, send the material to the publisher, and upload everything also the IACR server. Make sure authors have submitted the signed copyright forms (see Section 11).

$T-1.5$ Announce Rump Session Chair on your event webpage.

$T-1$ Notify the session chairs of which session they will chair, and contact the IACR Archivist (`archive at iacr dot org`) about the material that needs to be archived and how it needs to be submitted (see Section 11).

T At your event, you are responsible for the program (see Section 12).

$T+1$ Send any relevant materials to the Archivist, the Communications Secretary, the General Chair, and the Board (see the detailed timetable in Appendix C for what to send where), and archive everything for at least a year (see also Section 11).

4 Planning the Program

Overview. Consider how you want to run your event: invited speaker(s), special sessions (e.g. poster session? difference in schedule?), best paper award(s), rump session, how many submissions by Program Committee members are allowed and how those submissions will be handled, the various other Program Committee-related issues mentioned in the next section, and whatever else you may come up with. The Board encourages experimentation and new ideas, but any change which impacts the financial, publication, or local organization side of an event must be discussed with the Board first.

A Board decision in 2014, approved by a referendum in 2016, has decided to ask the Program Chairs and Committees of the three IACR General Conferences in 2015 "to have parallel sessions for a significant part of the program."

Submissions to all IACR Conferences must be open to anyone and never by invitation only. For General Conferences, the Board may have notified you that you have to schedule an hour for an IACR Distinguished Lecturer. Title and subject of his/her presentation are determined by this lecturer, from whom you have to obtain all relevant information (such as slides) to put on the IACR website after the Conference.

Invited speakers. Once your Program Committee has been selected, discuss invited speaker(s) with them. The choice of speaker(s) should be yours, with input from your committee, and should not be guided by pressure from other parties. Invited speakers are often invited to speak about a subject of your and your Program Committee's choice, but you may also leave the choice of topic to them. The invited speaker(s) and the IACR Distinguished Lecturer (if any) should be invited to contribute an abstract or a full paper to your event proceedings and may decline to do so.

IACR Membership meeting (General Conferences only). For the General Conferences you should schedule one hour for an *IACR Membership meeting*; typically this meeting is held immediately after the end of the sessions on Wednesday (before the banquet or the beach BBQ). The IACR President or his/her representative may also want to make a short announcement during the opening session of the Conference. For Area Conferences, you should consider to plan a short presentation on the IACR during the event.

Poster session. Some attendees can only receive from their funding agencies a grant to attend an event if they have a submission accepted. Some events have therefore introduced poster sessions. You may consider accepting submissions for a poster session if the submissions are of high enough value and if they can receive a proper display at your event site. You should coordinate with the General Chair to determine whether a poster session is feasible and desirable. If you choose to have a poster session, the decision to accept a submission for it should only be taken on scientific grounds.

Best paper award(s) and top three papers. The Board strongly encourages Program Chairs to select one of the accepted submissions to receive the best paper award and equally strongly encourages Program Chairs to select the top three papers (including the best paper) for invitation[1] to the Journal of Cryptology. It should also be considered to select a best student paper (make sure the criteria for a student paper are clearly defined).

It is not uncommon for funding decisions to be made based on such types of awards. Having them evens the battlefield with other branches of science where such awards are common. Keep this in mind while deciding if you want to give a best paper award (in principle — at a later stage you and your committee should decide if there is a paper that is worth this honor).

Be careful with conflicts of interest during the selection of the top three papers and the best paper award. It is likely that a substantial fraction of the program committee will have a conflict with one or more papers in the "longlist" of candidates (typically 5-8 papers). One procedure which worked well in the past uses two steps: in step 1 all Program Committee members are allowed to recommend papers (for which they don't have a conflict) to the longlist; in step 2 a subcommittee is selected without conflicts in this longlist; this subcommittee then chooses the top three papers and the best paper through a discussion and voting process.

The awards (including the top three papers invited to the Journal of Cryptology) should be mentioned in the foreword of your Conference proceedings and at your Conference during the introduction of the papers that received it. For General Conferences, coordinate with the President about organizing and handing over a certificate for the best paper. A financial award should not be provided.

Rump session. Current practice is for all IACR Conferences to have a rump session during one evening of the event, to present recent developments, announce upcoming events, and to have fun. Prior to your event, choose a person to chair the rump session, with whom you determine how rump session submissions are handled (including submission deadline, usually during the event itself) and submissions are selected (usually by the Rump Session Chair and possibly yourself). Remember, and remind your Rump Session Chair, that rump session submissions can be rejected. You may consider doing so to avoid known-to-be-bad repeat-performances. Aim for

[1] Except for the Conference/Journal hybrids.

a rump session that lasts at most 2.5 hours. Put all relevant information on the event website and make sure that the program and the presentation material are available online afterwards.

Submission and paper format and length. For continuity among the Conferences, the Board strongly recommends that submission are formatted in the same way as they will appear in the final accepted version. This should make it transparent to readers, as well as to reviewers, that the published version and the reviewed version correspond to each other in length and scope.

For Conferences with proceedings published in Springer's LNCS series, the CFP should include this requirement on formatting the submissions as follows:

> Submissions must be at most 30 pages using the Springer LNCS format, including title page, references, and figures. Optionally any amount of clearly marked supplementary material may be supplied, following after the main body of the paper or in separate files. However reviewers are not required to read or review any supplementary material and submissions are expected to be intelligible and complete without it. The final published version of an accepted paper is expected to closely match the submitted 30 pages.

For General Conferences, you must not deviate from this principle and from the formatting requirement unless the PC Liaison Officer agrees to it.

Note that as of 2015 Springer LNCS volumes will place any section in a paper called "appendix," which appears after the bibliography, to a place before the bibliography. Thus it makes sense to educate authors to call the matter after the main body and the bibliography the *supplementary material* and not the *appendix*.

Submissions by Program Committee members. For General Conferences it is recommended that a PC member is single author for at most one submission or co-author for at most two submissions (not both). The Area Conferences have their own policies which are usually less strict, such as at most two accepted submissions per PC member: best check with the Steering Committee or with the Program Chair of the previous year. As Program Chair you cannot (co-)author a submission. In particular, for Conferences that use the co-chair model, no Program Co-Chair can (co-)author a submission.[2]

It is recommended that PC member papers are kept to a higher standard than the other submissions. Generally this is achieved by assigning submissions (co-)authored by PC members to five or six reviewers, as opposed to the customary three reviewers for other submissions.

Dealing with unsolicited advice. Your *scientific* choices and decisions while planning your event should be based on your own sound judgment, possibly with input from your committee members, members of the Board, or others from which you seek advice.

If you feel that you are unduly guided or pressured one way or another by anyone — including your General Chair — you should ask the PC Liaison Officer of the IACR or an appropriate other member of the Board or the Steering Committee for assistance.

[2]The FSE Steering Committee has approved an exception: the Program Co-Chair can submit one paper per year.

5 Program Chair and Committee Selection

Program Chairs of IACR General Conferences are selected directly by the Board. This appointment should be made about 18 months before the Conference takes place. Program Chairs of IACR Area Conferences are recommended by their respective Steering Committees and approved by the Board. The structure of each Conference (specifically the possible use of co-chairs) is decided by the responsible Steering Committee.

The Program Committee (PC) of an IACR General Conference should be able to address the full range of research in cryptology; both theoretical and applied. The PC of an IACR Area Conference should have broad expertise within the Conference's area of emphasis together with sufficient experience in other areas of cryptographic research to provide context for submissions that might cross between sub-disciplines. The PC should typically represent all major geographic areas. Committee members should be competent, fair, reliable, and qualified professionals dedicated to research and having a wide range of interests and backgrounds — academic/industrial research, theory/applications, experienced/young. Other selection criteria: access to external reviewers (e.g., postdocs, senior PhD students), not the same people on too many committees in a row (but at least one member of the PC of recent IACR events may prove helpful).

To make sure you do not forget anything in the selection, you should run your initial choice past the PC Liaison Officer (and Steering Committee Chair). This is to simply check that all above aspects are covered, and for the corporate memory of the PC Liaison Officer to be applied, as he/she is also a member of the IACR Ethics Committee. For example there may be issues with some PC members which you may not be aware of from previous meetings.

Size of the Program Committee. Base the size of your PC on the number of submissions you expect for your event (based on previous years and the geographic location where it will be held) and the recommendation that each PC member should review between 15 and 25 submissions. If the number of submissions turns out to be much larger than expected and the reviewing load would become too high, the PC can be enlarged by a few members.

Finding PC member candidates. Recommendations of previous Program Chairs, the Program Chairs contact of the IACR, and other members of the Board, are helpful to identify suitable candidates. A list of past members and of recommended new blood can be obtained from the IACR Secretary. Young, but sufficiently established people are often more dedicated and enthusiastic than more senior people, but on the other hand are often more likely to accept papers which show technical brilliance over papers which will have lasting impact. Thus a balance in ages is a good idea. It is not uncommon that Program Chairs are contacted by volunteers eager to serve on the committee or by people making unsolicited suggestions whom to invite. Such requests and recommendations can safely be ignored. It is an exception that PhD students serve.

Establish rules for the PC. When inviting people to serve on the PC you should inform them upfront about all relevant aspects of the process as you intend to run it and that may influence their decision to accept your invitation or not:

- the decisions you have made while planning your event, including your decision on the submission and paper formats;

- the phases of the reviewing process;
- the time commitment the PC members will have to make (the equivalent of at least two to three full weeks working time);
- that the submissions for the IACR General Conferences must be anonymous to PC members throughout the reviewing process; authorship should only be disclosed by the Program Chair in rare instances involving conflicts or other special circumstances;
- if the PC member reviews will be anonymous with respect to each other (usually they are not);
- whether you will have a physical PC meeting (it varies; see below);
- how many submissions by PC members are allowed and how they will be handled (e.g., more reviewers, maybe held to higher standards);
- how conflicts of interest are defined and will be handled (see Section 7 for more details);
- the PC members' responsibility to act in an ethical way, including informing the Program Chair if they are inadvertently asked to review their own submission or any other submission for which they have a conflict of interest;
- the PC members' responsibility to select competent external reviewers (if so desired) and to inform these subreviewers of the paper selection criteria (see Section 9);
- any other decision you made that may influence the acceptance of prospective PC members.

Keep in mind that the responsibility for the program lies with the PC and ultimately with you as Program Chair. It is not necessary to run the PC as a democracy and you will have to decide if consensus cannot be reached. On the other hand, it is often better to work by consensus.

Keeping PC members informed. Make a clear record of whom you invite and of their responses. It is not uncommon for people to forget they have accepted. It is therefore a good idea to regularly schedule a "liveness test" for your committee members between their acceptance and the start of the actual PC member activities. Keep everyone who has accepted to be on your PC informed of any decision you may reconsider and change: they may desire to opt out if the change is not to their liking. In any case, try to avoid having any of your PC members be surprised by any aspect of the way you are running your event.

Advisory Committee and Advisory PC members. For the General Conferences, the Program Co-Chairs of the coming year must serve as regular members of the program committee of the current year. In order to maintain the memory of the review process, the Program Co-Chairs should compose an Advisory Committee consisting of the Program Co-Chairs of the previous year and the coming year of the Conference. The Advisory Committee should be consulted for key decisions, including the composition of the program committee, the call for papers, the organization of the paper assignment, the organization of the review and decision process and the selection of invited speakers.

For the other Conferences, it is *suggested* that Program Chairs of the same event in the previous and the coming year (if selected already) are invited to be full or advisory members. Advisory members have full access to the information exchanged during the reviewing process but are not expected to contribute to the reviewing or decision process.

Physical PC meeting? Since the web-review software is in use, it can be argued that a physical PC meeting is not needed anymore and in fact a purely web-based decision process may be better. Some arguments are:

- All committee members can take part, usually even when they are traveling.
- All the previous discussion is available and can be conveniently referred to by everyone.
- All decisions can be made over a reasonable time period, with the opportunity to consider all the arguments and look up any references.
- There is less chance (though still possible) for one or two strong personalities to dominate the discussion. *Ad hoc* decisions are less likely to occur than at a physical meeting.
- Time savings and environmental issues.

On the other hand, there are also arguments in favor of a meeting:

- It is easier for PC members present at the meeting to get informed about and involved in decisions and discussions on submissions which they have not reviewed. This results in a more uniform application of decision criteria.
- It may be more time efficient, especially if the PC meeting can be co-located with a related event.
- It is much more fun.

If you have a physical PC meeting, each member should be given a chance to attend. You should encourage them to pay for the trip out of their own resources, but if this is not possible, you should reimburse (part of) their trip expenses from your budget which you must have negotiated with your General Chair. Financial support should not be a criterion for selecting PC members. Select a procedure for the PC meeting before the meeting. At the meeting, announce the procedure and stick to it.

6 Administrative Software

For IACR meetings you must use the WebSubRev software[3] written by Shai Halevi and hosted on the IACR server. This software is well-suited to the idiosyncrasies of IACR Conferences and it integrates into IACR's publication workflow process, which handles copyright.

Documentation, a demonstration, and source code for WebSubRev are available at `http://people.csail.mit.edu/shaih/websubrev/`.

[3] At the time of writing (March 2020), IACR is developing support for HotCRP; integration with the IACR publication workflow is ongoing.

The submission deadline should be chosen such that a human operator is present to monitor the final, say, two hours of the submission process. Although access will dry up almost completely within minutes of the deadline, it will be intense in the hour before, and a soft landing should be provided so that submissions will not be excluded because they were competing for bandwidth. Nevertheless, be strict.

Make sure well before reviewing starts that you and all your PC members can access and use it. It is recommended that you check the semantics of the grades and adjust them to your needs. Inform your PC members that they should not share their access credentials with the subreviewers or anyone else.

7 Call for Papers and Schedule for Submissions

You should draft the Call for Papers (CFP), send it to the General Chair, and make sure that the final version is put on your event website and on the IACR Calendar of Events prior to your event: about 11 months before the IACR General Conferences and about 8 to 9 months before the IACR Conferences. The CFP should include the topics of interest and what types of submissions are desired. It has more or less reached a *de facto* standard and it is most convenient to modify a previous CFP, using the same format. Be explicit about the rebuttal conditions and timing. The IACR logo is available at `http://www.iacr.org/docs/`.

Statement on parallel submissions. There is a persistent problem of parallel submissions of essentially identical submissions to multiple conferences, workshops with proceedings, or journals. This is not allowed, as described further in the IACR policy on irregular submissions. Recent CFPs therefore include the following text:

> IACR reserves the right to share information about submissions with other Program Committees.

The CFP should also clearly state how parallel submissions to journals are handled. For copyright reasons a paper must not appear in an IACR venue and a journal without a substantially extended version being in the journal. A sensible approach is to impose that authors notify Program Chairs about parallel submissions to journals. Current online submission systems allow for the possibility to let authors tick a box indicating that they follow your policy regarding parallel submissions.

Anonymous submissions. Since 1990, submissions to IACR General Conferences have been anonymous (blind), with the exception of Crypto 2006 and Eurocrypt 2007. In the 2006 ballot, the IACR membership has approved with a strong majority the following policy on anonymous submissions and review:

> Submissions to IACR Conferences should normally be anonymous to program committee members throughout the reviewing process; authorship should only be disclosed by the Program Chair in rare instances involving conflicts or other special circumstances.

You must abide by this anonymity policy and this policy should be stated in the CFP. This policy is recommended but not mandatory for IACR Conferences; Program Chairs for Area Conferences should check with the Steering Committee.

Submissions (co-)authored by PC members. You may also state your policy about submissions by PC members (see Section 4).

Conflicts of interest. The IACR has a Policy on Conflicts of Interest (COI) for program committee members and sub-reviewers of papers (`http://www.iacr.org/docs/conflicts.pdf`). All General Conferences must comply with this policy. If any Area Conference chooses to follow an alternative Conflict of Interest policy, that policy must be documented publicly and approved by the relevant Steering Committee.

The IACR COI policy states that a reviewer has an automatic COI with an author:

1. if one is or was the thesis advisor to the other, no matter how long ago;
2. if they shared an institutional affiliation within the prior two years;
3. if they published two or more jointly authored works in the last three years; or
4. if they are immediate family members.

A reviewer has an automatic COI with a submission if he or she has an automatic COI with any of its authors. Additionally, a reviewer has an automatic COI with a submission if the reviewer is authoring a paper (in submission or in preparation) whose content substantially overlaps that of the submission. Check the IACR website for updates on this policy.

Authors can mark PC members they have a COI with when submitting their paper. Program chairs should verify that sufficient expertise remains among the reviewers who do not have a COI (in the case that authors would indicate too many conflicts).

Dates. The CFP should contain submission deadline and notification date (at least 6 and 3.5 months prior to your event, respectively), and the schedule for authors of accepted papers (such as due date for the proceedings version of their submissions). For the submission deadline, avoid specifying a time of day that allows ambiguous interpretation such as "12:00 PM" and mention the time zone. You can determine your own schedule by counting backwards from Springer's hard deadline for your event (Section 11). Please be aware that some authors need a notification of acceptance before they can apply for a visa, hence shifting this notification too close to the conference may be a problem.

In setting the schedule for submissions and the committee's work, consider the schedules of previous IACR events. Schedules of Conferences, including non-IACR ones, depend on each other, with submission deadlines of a non-IACR event often closely following the notification date of an IACR event. It is therefore not recommended to change the notification date once it has been announced in the CFP.

Other CFP issues. Any special requirements, such as your decision (Section 4) on submission and proceedings paper formats, should be clearly stated in the CFP.

8 Reviewing Process

IACR has issued guidelines for reviewers `https://www.iacr.org/docs/reviewer.pdf`. Please read these carefully and make sure your Program Committee members are aware of them.

Communicating with your committee. At any time during the reviewing process be responsive to all parties involved. Make sure you inform your PC members if you are out of touch for an extended period of time. Throughout the reviewing process, consistently use the same communication method to send messages to your entire committee. This can be email or the discussion facility of the web-review system. Do not use email for some and the discussion facility for other important messages, since PC members may miss them and fail to respond in time.

Confidentiality. The whole reviewing process and all submissions must be kept in confidence to the PC. This rule must only be relaxed with your approval and in well-defined cases, as described in this document and in the IACR policy on irregular submissions.

Initial processing. Once the submissions have been received make sure that anonymity is not breached by title pages, PDF hidden information, or other "features". If needed edit the submissions or request properly anonymized versions from the authors. You may indeed decide to reject those submissions which do not meet the submission criteria.

Make the resulting submissions available to the committee members through the web-review system, and give them a few days to indicate their reviewing preferences. Spend those days glancing through the submissions, to get an idea of the general quality and how well the various areas are covered, while trying to identify submissions that have been submitted to other Conferences or workshops.

Assigning the submissions. One of your most important tasks is assigning submissions to the individual PC members. The web-review system offers an automated assignment procedure based on the PC member's preferences and expressed areas of interest. As helpful as this may be, you are responsible for the final assignments and this involves manual labor. Make the assignments based on the PC members' preferences and areas of interest (as expressed by them using the web-review system).

Consider assigning the entire responsibility for handling submissions for which you may have a conflict of interest (such as by your students or subreviewers) to another committee member. Each submission should be reviewed by at least three committee members who can be expected to have a reasonably high level of confidence in their reviews, at least one of which should be an expert and at least one of which should be a relative outsider to the submission's subject.

To help assess relative merits it helps if all submissions on a similar subject have overlapping reviewers. Attempt to avoid conflicts of interest by not assigning submissions to friends, colleagues, students, or PhD advisors of any of the authors. Assign submissions from committee members to as many reviewers as you decided upon when planning your event (see Section 4).

Irregular submissions. You should enforce the IACR Policy on Irregular Submissions `https://www.iacr.org/docs/irregular.pdf` and consult with the IACR Ethics Committee (chaired by the Vice President) if you discover any substantial violations. Irregular submissions typically fall in two categories:

Parallel submissions: A parallel submission occurs when authors submit essentially the same material to one or more other events with overlapping reviewing periods. They may be identified at any time during the reviewing process. Ask your PC members, in particular

those serving on other Program Committees, to be on the look-out for such submissions. They should be rejected. The authors of parallel submissions should be told about the rejection only at the final decision time when all other authors get notified. The Program Chair(s) of the other event(s), however, should be notified as soon as the double submission is identified.

Plagiarism: Occasionally, substantial parts of existing publications are submitted, virtually unchanged and without the addition of new material, by other "author(s)". In such cases, the IACR Ethics Committee must be involved and harsher action than a simple "reject" could be appropriate. Since establishing beyond doubt which party is responsible is probably beyond your and the IACR's competence, care should be taken.

Actual reviewing. The reviewing consists of the following phases, supported by the reviewing software (also refer to $T - 6$ through $T - 3.5$ in Appendix C for further suggestions):

Phase 1: Individual reviewing. Each reviewer should grade (1) the quality of a submission and (2) his or her confidence in the grade, and should give detailed comments about the submission.

It is the responsibility of each PC member to review the submissions you assign to them and to return the reports to you (or enter them in the web-review system) by the deadline. Reviewing can be delegated by a PC member to external reviewers, but the responsibility remains with the PC member. PC members should enter all reviews themselves in the web-review system and, to avoid breaches of confidentiality of the reviews, not share their access credentials with their subreviewers.

The comments in the report should be divided into three sections: comments for you, comments for the entire committee, and comments intended for being sent to the authors (duplication can be avoided). As the reviewing process progresses, these comments should be revised. For instance, a reviewer who dislikes a submission, but is convinced later by the other PC members that the submission is good, should revise the report before it is sent to the authors.

To obtain independent opinions about each submission, there is no interaction and discussion among the reviewers during phase 1.

At the end of this phase make preliminary decisions putting submissions with consistently high (or low) scores with sufficiently high confidence in the "maybe accept" (or "maybe reject") category, while putting the others in "discuss."

Phase 2: Rebuttal. IACR Conferences have been following the new tradition in the computer science community to give authors the opportunity to respond to the comments in a (brief) rebuttal. This can be helpful to point out factual errors in the reviews, to resolve misunderstandings, or to better understand the impact of a shortcoming in a paper. It may also help weed out unfair comments. There seems to be a consensus that this improves the quality of the review process for a moderate increase in workload.

If rebuttals are used, it is even more important that all reviews are returned on time; otherwise some authors may be treated unfairly as they do not get the opportunity to respond to all the first round reviews. It may be helpful to have a short discussion phase among reviewers before the rebuttal in order to resolve some conflicting comments.

Reviews with strong criticism may result in a withdrawal of the paper during the rebuttal phase. You may also decide to issue early rejects after the rebuttal period. This has some advantages, but also presents the risks that authors may use the quick first review phase as an oracle before submitting elsewhere.

Phase 3: Discussion. Give the PC members access to your preliminary decisions and to each others' reviews. Authors among them should not be given access to any information related to their submissions. Also, reviews and discussions should be made invisible to PC members if you feel that there is a risk of conflict of interests.

Ask the committee members to check carefully the preliminary decisions you proposed and to oppose if they do not agree. Ask all committee members to look at borderline submissions. For controversial submissions (those that received both high and low grades and thus ended up in "discuss"), ask the involved reviewers to sort out their conflicting opinions, and possibly assign further reviewers. For submissions with low overall confidence values you should assign the submission to further reviewers. During this phase, the committee should use the discussion feature of the web-review software to communicate.

It is absolutely necessary that you take an active role during this second round and force reviewers to respond to other reviewers' comments and contributions to the discussion, to make precise why they support or dislike a submission, etc. Many reviewers tend to be quite passive unless asked explicitly to make a statement regarding a submission. Sometimes it is necessary to be harsh with lazy reviewers.

It is also necessary to remind your PC that discussions on submissions should take place in the open forum as provided by the web-review software, and that it is inappropriate for them to engage in "private" email or other discussions behind others' (and your) back.

Often small flaws are found in interesting submissions. If these are not resolved during the rebuttal phase, you may consider contacting the author(s) to see if a technical flaw can easily be corrected or if a "gap" in an argument can be filled with some additional clarifications. In general authors are very responsive to such requests. If the review software allows for direction communications between authors and PC members, you should monitor and manage this carefully. An option that gives you more control is that you take the role of intermediary.

Discussions can get heated especially when the PC members cannot reach agreement. It is not uncommon that outside arbitrators, i.e., specialists in the field of the contentious submission that are not on the PC, are asked to give their opinion. You should contact these arbitrators after agreeing with the warring parties about the procedure that will be followed and whom you should ask.

During this phase gradually move submissions for which no new issues are brought forward from the "maybe" categories to the corresponding "accept" or "reject" category, and move submissions for which a clearer picture emerges from "discuss" to the appropriate "maybe" category. Solicit feedback on your moves, and do not hesitate to reconsider them.

Phase 4: Final decisions. At this point a reasonably clear picture should have emerged, with not too many submissions (ideally not more than about 50) still in the "discuss" category. Initiate a discussion among the entire committee to reach final decisions. If a physical PC meeting is held this is done during that meeting. Otherwise, use the web-review system to

engage the entire committee in active online discussions. Also, in this case you may want to devise an online voting mechanism to reach final decisions.

Schedule your and your committee's work in such a way that decisions are finalized well before the notification deadline, and such that submissions are moved between the categories in an orderly fashion that is properly discussed and agreed upon by your PC members. At the end of the process the two "maybe" categories and the "discuss" category should be empty, and a majority of the PC should support the final decisions.

If there is no physical PC meeting, decisions on PC member submissions are taking place as for other submissions, where the web-review system is used to exclude the author(s) from the discussions on their submission. With a physical PC meeting the PC member submissions can be handled before or after all other decisions have been made. If you handle decisions before the other decisions but do not communicate them to the PC members involved, they will be more relaxed during the rest of the meeting. It may be better for a balanced decision to handle the PC member submissions during the meeting at the time when the submission would be discussed if it were not a PC member submission, and to ask the author(s), if present, to leave the room when their submission is discussed. In all cases it is helpful not to fix a target number of submissions to accept (see Section 9).

For each submission there are four possible outcomes: accept, conditional accept ('shepherded'), proposed to be merged with another submissions (and possibly shepherded), or reject. Agree with the shepherds of shepherded submissions on the terms of acceptance and on the way the shepherding process is organized (with you as proxy between shepherd and author(s), or via direct communication between shepherd and author(s)). It should be realistically possible for the author(s) of shepherded submissions to fulfill the terms of acceptance of their submission(s). For mergers: set a clear policy in advance of the conditions (e.g., what happens if the authors of one paper disagree).

If you decided to have a best paper award, decide with your PC members which accepted submission should receive it, if any. You may consider excluding PC member (co-)authored papers from consideration for the best paper award; if included they should be held to a higher standard.

Ethics. Several previous Program Chairs have reported observations of unfair or unethical behavior by some committee members, especially for pushing the submission of close friends. Be aware that such things can occasionally happen and do not hesitate to stop them. In difficult cases, especially if it seems likely to result in harm to the reputation of any of the disputants or the IACR, contact the IACR Ethics Committee.

9 Selection Criteria for Papers

Acceptance rate. The IACR Conferences have reached a high standard and, as a consequence, quite a low acceptance rate ranging from below 20% to 30%. It can be expected that the acceptance rate will stay in this range, although the average quality of submissions has increased over the years. You should communicate to the PC a policy about how the total number of accepted submissions will be determined. Obviously, the number of accepted submissions should approximately match the number of slots you intend to fill. But avoid fixing an explicit

target for the total number of accepted submissions, also to facilitate discussion of PC member submissions.

Main acceptance criterion. The most important criterion for accepting a submission is its overall quality. It will also depend on the number of submissions to be accepted, whether there is a desire to try to balance the number of papers in different areas, and the number of submissions on any given topic. In any case, it should be understood that the content and the presentation of the material in a paper should be at an advanced level.

General acceptance criteria. Criteria for selecting the set of accepted submissions include the following:

- Novelty: Does the submission contain scientific contributions that have not previously been published and which are novel to an expert in the field?
- Interest to the experts: A paper should be of interest to the experts in the field. There are papers, for example papers with mathematical results with little cryptologic significance, which are completely novel and correct but simply do not attract a cryptologist's interest.
- Correctness: The technical part of a paper should be correct. However, a few minor, correctable errors are not sufficient reason to reject a submission if the rest of it is correct and interesting.
- Completeness and clarity: Is the paper well-written and does it contain all the details of the solution?
- Quality of the presentation: Is there reason to expect the final version and the presentation to be of high quality? Will the paper be the basis for an interesting talk?
- Does the paper lead to new directions in cryptology, for instance by proposing new concepts? This may be sufficient reason to accept a submission, even if the technical contributions are not groundbreaking.
- Can the proceedings version of the paper be expected to meet the requirements (if any) as set forth in the Call for Papers?

Communicate all criteria to your PC members and ask them to communicate the criteria to their subreviewers.

Theory, practice, and scope. Cryptology is a field that ranges from deep theory to concrete applications. It is particularly fruitful that the gap between theory and applications is bridged by some of the papers. As a consequence there is always a trade-off between selecting theoretical papers and application papers, but there cannot be an ultimate rule for balancing between the two. You should keep in mind, however, that you are chairing a *scientific* meeting and that there are other means than this event for informing the community about the state of the art in applications. Mere progress reports on industrial projects and product-related articles should not be accepted. But high-quality papers that would fall within the scope of an IACR Conference should also be considered to fall within the scope of IACR General Conferences; similarly, high-quality papers that point out non-trivial flaws in widely deployed solutions (and/or solutions for such flaws) can strengthen the program.

10 Communication with Authors

It is recommended that you communicate with the corresponding author (confirmation of receipt, acceptance/rejection letter) by email or, in exceptional cases, by regular mail. Sample letters are given in Appendix B.

Sending notifications. All notifications (accept, conditional accept, merge, or reject) should be sent to the authors more or less simultaneously. Avoid sending them in batches, such as "easy" rejects one day, and the tougher nuts (i.e., rejected at the very last stage of the discussion stage) the next day. Schedule your activities in such a way that there will be no notification delays.

Feedback for authors of submissions. It is strongly *suggested* to send to the authors as much information obtained from the reviewers as possible, especially for rejected submissions. It has been observed that fewer complaints are received if feedback is sent a few days after the notification. Ask the reviewers to edit their reviews in such a way that the reviews do not contradict the decision and include as much material from the discussion phase as possible. You should make sure that rude, derogatory, or unhelpful remarks are removed before the reviews are sent to the authors. For shepherded submissions you or the shepherd should clearly communicate to the authors the terms of acceptance of the submission. Usually, the author(s) of shepherded submission are asked to submit a revision of their submission to the shepherd at least two weeks before the proceedings versions of the papers are due. During these two weeks the shepherd can review the revised version and if necessary further guide the author(s) to make additional changes. Shepherding and merging can be an intense process for you, the shepherd, and the author(s) involved. Avoid judgmental remarks, and make sure not to change the terms of acceptance in the course of the shepherding process.

The ratings given for the submissions may or may not be communicated to the authors. If they are, inform your PC members about it, and ask them to make sure the overall scores are inline with the decision (otherwise you risk upsetting authors of rejected submissions). Authors of rejected parallel submissions get no other information than "reject" along with some strong language that parallel submissions are not allowed.

Instructions for authors of accepted submissions. If the submission has been accepted, you should send the authors the instructions for the authors/speakers. This will include at least the following:

- Instructions about preparing the proceedings version of the publication and the procedure for submitting this material (Section 11);
- Instructions for the copyright and consent (Section 11);
- Time, date, and length of the talk, possibly the identity of the session chair, and instructions on where and when to meet the session chair prior to the session in which the paper will be given; and
- Instructions on the presentation material. Encourage speakers to copy their presentation well in advance to the central computer used for the presentations at your event and to test that they display properly. If they need their own laptop, make sure that they test

the setup well in advance. You may instruct the speakers to use sufficiently large fonts and to make appropriate use of colors. If there will be a practice room, indicate it in the letter.

Dealing with complaints. Sometimes authors of rejected submissions get upset and complain to you, to your PC members, to members of the Board, or to other members of the community. This happens in particular when the authors feel that the reviewers have not done a sufficiently thorough job, for instance by not reading the complete submission. Dealing with such complaints is unpleasant. Obviously, they are best avoided by making sure that reviews are accurate (since you cannot be expected to read all submissions entirely this is the responsibility of the reviewing PC members) and that rejections are not based on arbitrary arguments (this is your job). Despite all precautions, there will always be complaints. You (and not your PC members) should deal with the complaints to the best of your abilities, possibly by soliciting additional feedback from your committee. However, decisions should not be reconsidered once notifications have been sent to the authors. The decisions are your full responsibility: it is the policy of the Board not to interfere with Program Chairs on these matters. Note that the Ethics Committee is not an appeal body for rejection decisions; the Ethics Committee deals only with complaints about unethical behavior.

Information for the General Chair. Send the list of titles and authors of the accepted submissions to the General Chair. Depending on your assessment of the situation shepherded submissions may or may not be included, with or without the name(s) of the author(s). Agree with the General Chair on a policy for giving grants to students. Finalize the detailed schedule, taking into account constraints provided by the General Chair and (for General Conferences) the membership meeting.

11 Proceedings, Copyright and Consent, and Archiving

Proceedings. Proceedings of the General Conferences and the Area Conferences PKC and TCC are published within Springer's Lecture Notes in Computer Science series. They should be available at the event. As IACR has an agreement with Springer that covers publication of these proceedings, no special procedure is needed. The contact at Springer is:

LNCS Editorial Office, Springer-Verlag
Computer Science Editorial
Tiergartenstraße 17
D-69121 Heidelberg, Germany
Tel.: +49-6221-487-8706
Email: `lncs@springer.com`
Web: `http://www.springer.com/computer/lncs`

Springer needs the final version of each paper and all other material that will be printed in the proceedings (such as the foreword, which you have to write) at least ten weeks prior to the event— contact Springer about the schedule). Your task is described by Springer's "Information for LNCS Volume Editors" available online. Collect the source files of final versions from all authors using WebSubRev and send the collection of sources to Springer along with the email

addresses of the corresponding authors. Springer will send the versions as they will appear in the proceedings (i.e., after last-minute formatting done by Springer) to the authors directly. Check with Springer that they received all papers. In the course of this process, handle the copyright transfer as set forth below, and do not pay attention to an occasional message from Springer referring to Springer's own copyright forms. Finally, you must retain the tex/latex/pdf files of all papers and front matter as submitted to Springer according to the paragraph on "Archiving" further down.

Typically the Program Co-Chairs or the single Program Chair are editors of the proceedings volume.

Printed copies of the proceedings are no longer included with Conference registrations; participants can explicitly request and pay for a copy that will then be sent by mail to their preferred address; there is no guarantee that this copy will arrive before the event. IACR members and Conference attendees have online access to the proceedings; this may be available already before the event starts.

Copyright and consent. Authors of a paper must assign the copyright in the paper to the IACR. This allows the IACR to publish the paper, and make sure it gets archived for posterity. No paper should be published without obtaining a proper assignment of copyright as described in IACR's Copyright and Publication Policy. This transfer is performed via the WebSubRev system when an author uploads their camera-ready version.

Note that, sometimes, Springer employees may send you standard instructions to use the Springer copyright forms and to send the originals to them. Please ignore these instructions (cf. supra).

The IACR Copyright and Consent form also requests authorization to distribute the slides and a video recording of the presentation. It also offers the opportunity to provide a license to distribute auxiliary information such as software accompanying the paper.

Authors must approve the transfer of copyright and the distribution of slides and video recording in the IACR copyright and consent form. Exceptions can only be authorized by the IACR President. This must be reflected in the Call for Papers.

Archiving. The IACR, as copyright holder for the materials submitted by authors, is responsible for retaining the material in its own archive. This includes all source material for the technical papers and the front matter. As the papers have been managed through WebSubRev, then the archiving process is easy, as the authors must upload their versions through WebSubRev. In addition, you must upload the front matter files (preface and indices as embodied in tex, idx, and associated files) through WebSubRev as well. Once this is complete send an email note to the archivist stating that the proceedings are ready for copying to the archive.

The IACR strongly encourages that authors upload a version of their LNCS paper to the Cryptology ePrint Archive as soon as possible. Details of how authors should do this, what version to upload, and the relevant IACR copyright notice are included when the authors sign the copyright agreement. If authors fail to do so, papers are uploaded automatically.

12 Before and at Your Event

You remain responsible for the program during your event. Therefore you should be available when problems arise (e.g. if speakers do not show up or if sessions have to be moved because of technical problems). Of course, this responsibility is shared with the General Chair. It is customary for the Program Chair to present entertaining statistics about the submission and reviewing process. This can be done during the membership meeting (if there is one), the rump session, or at the opening of your event.

Facilities. Check the event facility, the overhead projectors, the audio equipment, and computer projection facilities (computer with PowerPoint, PDF viewer, preferably English operating system, no chopped off margins). A pointer should be available. Make sure that there is a backup for everything (even the power cables).

Session chairing. It is recommended that the session chair meet with each author for that session. This meeting can take place during the first cocktail party or at lunch or breakfast prior to the session. The session chair should explain that each talk will be timed and that it is important to keep on schedule. The session chair should also encourage speakers to copy their presentation to the event computer well in advance of their presentation; if they are using their own laptop, the setup should also be tested well in advance. The session chair has the responsibility to keep the speaker within the time limit. The session chair will direct the question and answer time after each author's presentation. The session chair may promote questions and ask relevant questions if there are not any from the floor.

Videos from talks. The collection of videos of Conference presentations has started in 2013; Since 2016 recording and publication of video and presentation occurs by default under a creative common's license (cf. Copyright and Consent).

Kevin McCurley maintains a YouTube channel with videos of talks from IACR Conferences, and they are being archived on `http://www.iacr.org` for future distribution. See `http://www.youtube.com/TheIACR`. The most important part of planning for this is to make sure that the video production people produce one video per talk, because editing the videos after the fact is very time-consuming. The exact format is less important, and you can choose from whatever is available at the venue. In past years we have tried several formats, including

- A format where a camera operator moves between the speaker and the screen. See `http://www.youtube.com/watch?v=rJIlMPu9ndE`
- A format where only the slides are shown. See `http://www.youtube.com/watch?v=8CfJmSGXSTc`
- A format in which both speaker and slides are shown in a split view. See `http://www.iacr.org/workshops/pkc2010/02_constant_size_ciphertexts_in_threshold_attribute-based_encryption/`

Any of these formats are acceptable.

Presentation Materials. The presentation materials must be collected and distributed via the website under a creative common's license (cf. Copyright and Consent).

13 Budget, Finances, and Reporting

Budget. It will be necessary for you to prepare a proposed budget for the expenses that will be incurred by you and the Program Committee. This must be submitted to the General Chair at least 8 months prior to your event. Please remember to get approval from the General Chair for any significant deviations from your budget before you make them. In any case, follow the instructions you receive from the General Chair. If you do not receive such instructions, contact him or her. Recall it is the General Chair who is responsible to the board for financial matters, and not you; thus all budget decisions must be approved by the General Chair.

Financial Report. Within three to four weeks after your event you must prepare a financial report for the General Chair. This report should include a list of all expenses and be sent along with all of the receipts to the General Chair. If you have paid directly for any of the expenses, the General Chair will reimburse you. However, for anything other than organization charges, the General Chair should be billed directly in order to keep your out of pocket expenditures to a minimum.

Confidential report for the Board. Around the same time, write a confidential report for the Board summarizing your experience with your PC members, the review process, your assessment of the outcome, your suggested changes to this document, and anything else you think the Board may find useful to be made aware of. A suggested structuring of this report is as follows.

General assessment. Report on the "big picture".

Major alerts. Report on any exceptional issues that required you or your committee to take unexpected action as part of the selection process.

Changes. Report on changes you made compared to the "usual" way of running an event and describe your experience.

Submissions. Report on numbers of submissions, accepted submissions, rejected submissions (including parallel submissions), and withdrawals.

Parallel and other irregular submissions. Report on the scale of the problem, any particular steps that you took to discover parallel submissions, and how you dealt with them.

Committee membership notices. Report on any members of your committee who demonstrated particular skills or commitment that you feel should be brought to the attention of the Board.

Author issues. Report on out-of-the-ordinary communications with authors, in particular on complaints that you have received from authors.

Guidelines comments. Report your proposed changes to the Program Chair guidelines.

Other issues. Report on anything else you feel the Board should be made aware of.

News report for the IACR website. Write a report on your event for inclusion in IACR News and send it to the General Chair. This report should not contain any confidential issues. It may for instance include the statistics you presented during your event, or any other non-confidential matter you see fit.

A More Information

More information is available on the IACR website at `http://www.iacr.org/` including:

- Guidelines for Reviewers;
- Guidelines for Authors;
- Policy on Irregular Submissions;
- Policy on Conflicts of Interest.

You should also obtain information about past Conferences. Do not hesitate to contact the members of the Board for more information.

The current members of the Board are listed at `http://www.iacr.org/bod.html`. You get to the Board of Directors area on the website when you remove the string `.html` from this URL. Important email addresses:

President	`president at iacr dot org`
Vice President	`vicepresident at iacr dot org`
Treasurer	`treasurer at iacr dot org`
Membership secretary	`iacrmem at iacr dot org`
Webmaster	`webmaster at iacr dot org`
Communications secretary	`info at iacr dot org`
Secretary	`secretary at iacr dot org`
Board	`bod at iacr dot org`
Archivist	`archive at iacr dot org`

B Sample Letters to the Authors

B.1 Rejection Letter

An example of a rejection letter is the following:

> Dear author,
>
> I am sorry to inform you that your submission _____ was not one of those accepted for CONFERENCE.
>
> The review process for CONFERENCE has been a challenging and delicate task for the Program Committee. Each paper was carefully evaluated by at least three reviewers. The work was very difficult because of the large number of high quality papers which were received and the relatively small number which could be accepted. There were ___ papers submitted and only ___ time slots available for presentations.
>
> The Program Committee members have put in a significant effort in order to provide useful feedback to the authors, but due to time constraints, this was not always possible. If comments were made that we believe would be beneficial to the authors, they will be sent shortly.
>
> Thank you very much for submitting your work to CONFERENCE, and we hope to see you at the conference.

Sincerely,

NN
CONFERENCE Program Chair

B.2 Acceptance Letter

An example of the acceptance letter is the following:

> Dear author,
>
> It is our pleasure to inform you that your paper _____ has been accepted for CONFERENCE. Congratulations.
>
> Please confirm receipt of this email, and provide us with the (corrected) title and complete list and affiliations of authors (the submission server did not always retain this information). This will allow us to distribute the list of accepted papers. Please confirm that one of the co-authors will present the paper.
>
> The selection of the papers has been a challenging and delicate task. Each paper was carefully evaluated by at least three reviewers. The work was very difficult because of the large number of high quality papers which were received and the relatively small number which could be accepted. There were ___ papers submitted and only ___ time slots available for presentations.
>
> The Program Committee members have put in a significant effort in order to provide useful feedback to the authors, but due to time constraints, this was not always possible. However, we expect that you do your best to take into account any comments received while producing the final version.
>
> Within a few days I will send you the comments and detailed instructions for preparing the final version (Springer's llncs style). In order to be included in the proceedings, the final version of your paper must reach us by _____. This is a firm deadline. Note also the strict length limit of __ pages.
>
> On behalf of the Program committee I would like to thank you for your submission and your support to CONFERENCE. I am looking forward to meeting you in ____.
>
> Sincerely,
>
> NN
> CONFERENCE Program Chair

For instructions to authors see Section 10.

C Detailed Timetable

The following timetable is an expanded version of the one given in Section 1. It contains some potentially useful reminders and suggests common sense approaches to a variety of issues. All times are in months from time T of your event. If the proceedings would be available only after your event, some parts of the timetable can be delayed a little. (Remember if your conference uses the parallel or rolling co-chair model, everything applies again to both co-chairs together.)

$T - 18$

- Read this document.
- If you have a co-chair, meet or call your co-chair and discuss your experience from past events and/or your expectations for this event.
- Talk to experienced people in the community about their experience as Program Chair or committee member. Try to obtain information about how Program Committees are run in other scientific communities in related areas.
- Make up your mind how you want to run this process. If you intend to implement major changes compared to how it is usually done, you may want to solicit feedback from the PC Liaison Officer, the IACR President and other members of the Board.
- Design a detailed plan and timetable of your job and the committee's work.

$T - 12$

- If you were invited as an advisory member of the Program Committee of the same event a year before the one you are responsible for, observe the process, consider what you would do differently, and what you could improve.
- Select the Program Committee (see Section 5). Inform the candidates that you invite for your committee about the reviewing process (see Section 8), the time commitment they will have to make, and of the way you intend to run the process before they decide whether or not to accept your invitation.
- Contact Springer about the publication of the proceedings and make clear arrangements and a time schedule for all contacts between you and Springer. Make sure the electronic proceedings will be ready before the event.
- Inform yourself about the electronic submission and reviewing software (see Section 6). Arrange an infrastructure to install, test, and run the submission system. Make binding arrangements if someone else runs it for you. Get help if needed. The submission server should be available at least three months before the submission deadline.

$T - 11$

- Make sure you have working contact information for all your committee members.
- Draft a Call for Papers (CFP; see Section 7). You can base your draft on the previous CFPs for the same event.
- Solicit feedback on the draft from the General Chair and the members of your committee, finalize the CFP based on their comments, and stick to the dates given in the final CFP.
- Submit your call for papers to the General Chair for publication on the event website and arrange how to announce it in other locations.

$T - 10$

- Ask each of your committee members to specify the topics in which he or she does or does not want to review submissions.

- Solicit input from your committee about invited speakers: how many, and whom to invite. Be aware that there may be an IACR Distinguished Lecture at your general conference. Invited speaker(s) or IACR Distinguished Lecturer may decide to have a paper in the proceedings.

$T-9$

- Decide whether or not you want to have a physical Program Committee meeting, possibly with input from your committee.
- Make sure the submission server is up and running.
- Finalize negotiation on the budget (See Section 13) with the General Chair.

$T-7$

- Make sure the reviewing software is up and running.
- Send usernames and passwords for access to the reviewing software to each of your committee members. Make sure that your committee members understand that they should enter all reviews themselves, including reviews by subreviewers, and that their access credentials should not be shared with anyone else (including their subreviewers).
- Check that all committee members can access the reviewing software.

$T-6$ First evaluation period.

- You should have the submitted papers by now. Initiate the reviewing process (see Section 8):
  - make the submissions available to your committee members so they can express their preferences;
  - based on their preferences and their lists of specified topics, assign the submissions to the committee members;
  - remind your committee members that from now until well after the reviewing all discussions about submissions between them and authors should be channeled through you;
  - make sure the committee members can enter reviews;
  - determine rump session policy, send it to the General Chair to be included in the event announcement/registration information, and announce it on the event webpage.

  At this point the first stage of the reviewing process starts. Usually, committee members cannot read each others' reviews at this stage.

$T-5$ Second evaluation period: the discussion phase.

- Once the majority of the reviews has been entered:
  - put submissions with consistently low (or high) scores of sufficiently high confidence in the "maybe reject (or accept)" category, but keep the others in "discuss";
  - give the committee members read access to all reviews (except for conflicts);

  - encourage the committee members to discuss the reviews with each other, in particular for submissions with diverging scores.
- While discussions are taking place:
  - monitor the discussions, encourage inactive committee members to participate and solicit more reviews where needed;
  - consider contacting authors in whose papers small flaws have been found after the rebuttal phase to verify if the problem can be fixed, and notify the reviewers of your initiative;
  - gradually move submissions from the "maybe" categories to the corresponding "reject" or "accept", replenishing the "maybe's" with submissions from "discuss" for which consensus is reached;
  - do not hesitate to reconsider your assignments;
  - be flexible, but make sure that a clear picture emerges.
- For the General Conferences, it is reasonable to aim for at most 80-100 submissions in "discuss" at the end of the discussion phase.
- Make up your mind how to make the final decisions: during the Program Committee meeting if there is one, or using some other well-defined process otherwise. Act transparently.

$T - 4.5$ Rebuttal period

- If rebuttals are used, the rebuttal phase should start 6-8 weeks after the submission deadline. Authors have typically 4-7 days to provide their rebuttal. Discussion continue after the rebuttal period.

$T - 3.5$ Final decisions.

- Decide for each submission if it will be accepted, conditionally accepted ('shepherded'), proposed to be merged with another submission, or rejected. Make sure that the shepherds know and agree which conditionally accepted submission they will be shepherding and agree with them on an interaction mode between shepherd and authors (directly or via yourself as a proxy).
- Notify authors of the decision (see Section 10). Ask your committee members to edit their comments for the authors within two or three days of author notification, and to include useful material from the discussion phase.
- Once you have made sure that the comments do not contain contradictory, unhelpful, or rude remarks, send them to the authors.
- Agree with your General Chair on a policy for giving grants to students. Note that all students who present papers receive a waiver for the registration fee from the IACR Fund for Student Presenters.
- Send the list of titles and authors of accepted submissions to the General Chair. As of 2017, this is now available as a JSON file export from WebSubRev, and this should be sent to the General Chair or webmaster.
- Finalize the discussion on invited speakers with your committee, and notify the General Chair of the speakers and topics.

- Decide, possibly with input of the committee members, on the best paper award/best student paper award as well as the top three papers that will be invited to the Journal of Cryptology. Notify the Editor in Chief of the Journal of Cryptology about these papers.
- Brace yourself for feedback from authors and other unpleasant surprises.
- Send instructions to authors of accepted submissions to prepare manuscripts for the proceedings. For shepherded papers you may want to act as proxy between authors and shepherds.

$T - 3$

- Ask the committee members for the names of all external reviewers.
- Appoint session chairs (committee members often volunteer).
- Determine the program schedule in collaboration with the General Chair in order to coordinate the technical and social programs (for General Conferences, take into account the membership meeting). There is now a tool at `https://www.iacr.org/tools/` to make this much easier, using the JSON file export from WebSubRev. The tool produces a JSON output format that populates the conference websites.
- Monitor the shepherding processes, if any.

$T - 2$

- Due date for final papers: make sure the authors send the versions of their papers as they will appear in the proceedings to you. Make sure you get the proceedings contributions of your invited speaker(s) and IACR Distinguished Lecturer, if applicable. Make sure you get a completed copyright and consent form for each paper that will appear in the proceedings.
- Write a foreword for the proceedings, including acknowledgments for all those who helped, in particular all the external reviewers, and mention which paper received the best paper award (if any) and which papers have been invited to the Journal of Cryptology (if any).
- Send all required material to Springer for publication of the proceedings.
- You must also hand over all material as submitted to Springer to the Archivist.
- You must ensure that electronic scans of completed copyright forms for all papers in the proceedings have arrived at the IACR Copyright Form Registry.

$T - 1.5$

- Choose the Rump Session Chair and announce this information on the event webpage.

$T - 1$

- Notify the committee members and session chairs of the program schedule and of which session they will chair.
- Contact the Archivist (`archive at iacr dot org`) to ensure that your material is properly retained. See Section 11 for detailed instructions.

T

- At your event you remain responsible for the program (see Section 12). You may want to say something about your experience during the IACR membership meeting, the rump session, or at the opening of your event.

$T + 1$ Closing checklist.

- Send electronic versions of all requested material to `archive at iacr dot org`.
- Send the list of rump session presentations, including authors and titles, to both `newsletter at iacr dot org` and to `archive at iacr dot org`.
- Submit the financial report to the General Chair (see Section 13) along with receipts.
- Send your contribution to the report of your event to be published in IACR News to the General Chair.
- Submit your confidential event report (see Section 13) to the PC Liaison Officer and the President.
- Archive all material for at least one more year (see also Section 11).
- Take a well-deserved rest.

D Best Practices

- Read this document.
- Be responsive and communicative.
- If you co-chair an event, establish a clear and open working relationship among the co-chairs.
- Establish a good working relationship with the General Chair, the PC Liaison Officer, and the Steering Committee Chair.
- Don't be judgmental in your communications to authors.
- Stick to the dates, once published.
- Be clear to all parties affected about the way you will be running your event.
- Don't hesitate to ask for advice.
- Read (and follow) the closing checklist ($T + 1$ in Appendix C).
- Abide by all the rules denoted by "must" in this document.

E Conference/Journal Hybrids

FSE and CHES have moved from a conference mode to a Conference/Journal Hybrid, with papers published in the IACR Transactions on Symmetric Cryptology (ToSC) and the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES). The main principles behind these journals are explained in the FAQs: `https://tosc.iacr.org/index.php/ToSC/FAQ` and `https://tches.iacr.org/index.php/TCHES/FAQ` and summarized below.

There are four submission deadlines and review periods per year; every quarter a new issue of the journal is published. The Conference program is composed of the papers accepted in the 12-month period ending 2-3 months before the Conference; presentation of the papers is mandatory. The Program Co-Chairs are also called Co-Editors in Chief of the journals.

Obviously some of the rules and guidelines in this document do not apply and some other rules and guidelines are necessary. This section lists the major differences. Information on timing is included at the end.

Rolling co-chairs (FSE). This section applies only to FSE that uses the *rolling co-chair model*. In this model one person is appointed as *Program Co-Chair for two consecutive editions of the same Conference*. During this time each Program Co-Chair serves in the first year as the "junior" chair and works with a "senior" chair who also served the prior year. In the second year of appointment, the Program Chair will function as the "senior" chair and work with a new "junior" chair. The "junior" and "senior" chairs should bear a comparable share of the workload. The terms "junior" and "senior" are only used informally to differentiate between the first and second years of appointment; the terms "junior" and"senior" should never be used for external communication. The names of the co-chairs must always appear together in all publications regarding the event: both should appear as co-editors in chief in the journal and on the Conference website. A *suggested* arrangement may be that "junior" chair defers to the "senior" chair for irreconcilable difference.

Planning the program. An important consequence of the hybrid model is that one does not know the total number of submissions for the Conference when deciding on acceptance. The experience is that more papers get submitted and accepted (sometimes after major revisions). This requires careful coordination with the General Chair, who may have to accommodate for more accepted papers (and perhaps parallel tracks).

A second difference is the selection of the best paper award: the recommended approach is to nominate a few candidates (or possibly none) for each issue, and to make the decision after the papers for the final issue before the Conference have been selected. It has been decided to not invite the top papers for the Journal of Cryptology.

In order to allow for a high quality review in a short time, the page limit (excluding bibliography) has been set to 20 pages in the corresponding template.[4] Longer papers (up to 40 pages) can also be submitted: in that case there is no guarantee that the paper will be reviewed for the current issue; the Program Chairs may delay the decision to the next issue in order to allow for a proper review.

Members of the Program Committee may submit one new paper per deadline[5] and resubmit

[4] See `https://github.com/Cryptosaurus/iacrtrans`; the amount of text on a page is larger than with the Springer LNCS format.

[5] It has been decided to drop this restriction as an experiment for CHES 2021.

prior submissions that received a major revision. For TCHES, Editors-in-chief are not allowed to submit papers (neither new ones nor revisions of prior submissions) during the four issues they are handling. For ToSC, one submission per year is allowed; this submission is handled by the other Program Co-Chair outside the webreview system.

Program committee selection. In the hybrid model, the review load is more evenly spread over the year. However, the time available for each review period is limited to two months. This means that the number of papers assigned in each round to a PC member for each issue should be at most four to five. As papers are also resubmitted after revision, more submissions will be received. It is thus recommended to make the Program Committee sufficiently large (40 to 50 members). Moreover, PC members should have the option to "opt out" for one of the rounds.

It is not feasible to have a physical PC meeting in the hybrid model.

Administrative software. The WebSubRev or HotCRP software must also be used in the hybrid model. As this software considers every issue as an isolated Conference, this requires some additional bookkeeping by the Program Chairs and the Program Committee members, in particular for long papers, that are reviewed for the next issue, and major revisions.

Review process. The reviewing process is similar to the one for regular Conferences with two main differences. First, the review period is more condensed: five weeks are available for Phase 1, one week for Phase 2 and only three weeks for Phases 3 and 4. The time from acceptance to camera-ready deadline is one month. This requires careful planning and full collaboration from the PC members

As the review process has a memory, five final decisions can be made.

Accept the paper as is.

Accept with minor revision: this corresponds to conditional accept (or 'shepherding') described in Phase 4 in Section 8.

Merge the paper with another submission.

Accept with major revision: the authors are invited to revise and resubmit their article to one of the two following submission deadlines (if they fail to do so, their submission will be treated as a new one). The authors should receive clear instructions on how to update their papers and which conditions need to be met. For consistency, the reviewers will typically be the same as in the first review, or there will be a strong overlap. Only one major revision is allowed for TCHES.

Reject: this means that the changes required for acceptance are so large that this is a new submission (e.g., adding major new results).

For minor and major revisions, it is essential that the authors receive clear instructions on the conditions for acceptance. This requires that reviews are written very carefully and contain constructive, complete feedback (to avoid the problem that new requirements are raised during the shepherding process or the second review). It is recommended to assign a lead reviewer during Phase 3 who is responsible for drafting these instructions in consensus with the other reviewers.

Proceedings. The IACR Transactions on Symmetric Cryptology and the IACR Transactions on Cryptographic Hardware and Embedded System are published online by the Ruhr University of Bochum (`https://tosc.iacr.org` and `https://tches.iacr.org/`). The license is a Creative Commons license (BY 4.0) that allows for Gold Open Access. There are no costs associated with publication in these journals.

The transactions expects its authors to submit camera-ready manuscripts. Authors who need professional copy-editing or other production services should seek outside assistance before submitting to the journals. Hence authors need to make sure that typesetting is of high quality and that references are standardized and clean. A LaTeX template has been created for the journal.[6] The final check is performed by the Program Co-Chairs and the Managing Editor.

As the journal version is the final version available in Gold Open Access, there is no need to upload the final version of the papers to the Cryptology ePrint Archive and there is no automatic upload. Authors may still chose to do so at their own discretion.

Timetable. The timetables in Section 3 and Appendix C have to be amended as follows. The first submission deadline of the Conference in year N is 1-2 months before the Conference in year N-1, that is, in $T - 13$ (or $T - 14$). This means that the Program Committee should be selected in $T - 16$, the call for papers published in $T - 16$ and the submission server opened in $T - 14$ or $T - 13$. Hence items 2-6 need to be advanced by 4-6 months. Of course there are four submission/review cycles.

It is strongly recommended to make a detailed calendar starting with $T - 16$ and mark all important dates such as submission deadlines, rebuttal openings, notification dates, minor revision process. Please coordinate between co-chairs to make sure that at least one of you can dedicate sufficient time to the crucial moments.

A foreword spanning the one-year submission period of a Conference in the hybrid model should be published in the last issue published before the Conference takes place.

[6] `https://github.com/Cryptosaurus/iacrtrans`