IACR Guidelines for the Real World Cryptography Symposium

July 2017*

The purpose of this document is to help the Steering Committee of the Real World Cryptography (RWC) Symposium and the RWC General Chair run a successful symposium, and to help in managing the IACR finances and membership.

The RWC Symposium is organized by the IACR according to the Bylaws of the organization in a way that is similar to the IACR Conferences, but with notable differences. The RWC Steering Committee oversees the organization of RWC.

The guidelines evolved mainly from the procedures that seemed to work well for past organizers. For the most part, guidelines are not meant to be rigid but rather formulas that will help make things work; only a limited number of rules is listed in this document. Such rules can usually be recognized by the imperative "must."

If you are the General Chair of RWC then you must 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 IACR Board of Directors or the RWC Steering Committee beforehand.

At various points this document will refer to specific sections of other IACR guidelines. These sections are assumed to be included *verbatim* into this document; they are not included explicitly to avoid duplication of information. It will be *explicitly* stated where RWC differs from other guidelines of the IACR.

This document will continue to evolve. Please send your feedback and suggestions for improvement to the IACR Officers, the IACR Board of Directors, and to the RWC Steering Committee.

Nigel Smart (2017).

Contents

1   Real World Cryptography Steering Committee Bylaws

RWC mission statement:

To be the top-tier forum for discussion of the research and practice of applied cryptography, to build a strong applied cryptography community, and improve the security of computing in practice.

The RWC Steering Committee (from now on simply, the Committee) is a group of volunteers that oversee organization of the annual Real World Cryptography Symposium. Committee member responsibilities include:

- Finding locations and local organizers

- Deciding the format of the conference: percentage of invited vs. contributed talks and archival format (proceedings, recorded videos)

- Identifying, discussing, and ultimately sending invitations to potential speakers

- Identifying sponsorship opportunities and pursuing them

- Selecting Levchin prize award winners

- Managing relationships with other bodies

- Maintaining the website at `https://rwc.iacr.org/` in collaboration with the IACR webmaster

All decisions are made by reaching consensus, or, if necessary, by plurality vote of Committee members. Any Committee member can request a vote.

Contributed talks are "light-touch" reviewed by a separate program committee consisting of six invited reviewers, plus five members of the RWC Steering Committee. The chair of the program committee is selected by the Committee and approved by the IACR Board of Directors. The appointment is for a term of three years (with possibility for renewal). The primary criterion for invited talks is that the talk should be interesting to the RWC audience. Strong academic research results have other venues (IACR General Conferences and Area Conferences) and product descriptions also have other venues (RSA Conference etc). For more details see Section 13.

The organizational goal is to have the Committee consist of at least 5 and at most 9 members, a majority of whom should be research active. Ideally, each Committee member serves a 3 year term, at the conclusion of which the member steps down and is replaced by a new member. Achieving this in the short term is likely to be problematic as all Committee members are new. New members are appointed by invitation of the existing Committee. There are no term limits, meaning that someone can be re-invited back to the Committee, though this case should be exceptional.

The founding members of the RWC Steering Committee (Dan Boneh, Aggelos Kiayias, Kenny Paterson, Tom Ristenpart, Tom Shrimpton, Nigel Smart) are currently exempt from the requirement to step down after 3 years, for not creating too much churn early on. The plan is to phase the founding members out more slowly over time. New members of the Committee are expected to have expertise (industrial or academic) in cryptography, a wide network of

contacts in the community, shared vision in the mission of RWC, and good rapport with existing Committee members.

The Committee currently (2017) consists of: Dan Boneh, Aggelos Kiayias, Brian LaMacchia, Kenny Paterson, Tom Ristenpart, Tom Shrimpton and Nigel Smart. The current chair of the program committee is Dan Boneh (2018-2021).

2   Organizing the RWC Symposium

Include verbatim Section 1 ("Organizing an IACR Workshop or Conference") of the IACR General Chair guidelines.

In particular, the final authority for approving a symposium proposal resides with the IACR Board of Directors.

3   Timetable

The following timetable shows when key tasks should be completed. All times are in months from time T of the symposium. This timeline is specific for RWC.

T−18 A proposal by the General Chair for dates, venue, organizing committee, and a preliminary budget should be sent to the Committee.

T−13 The proposal will be selected by the Committee and approved by the Board.

T−12 Confirm the meeting place as soon as the Board has approved your proposal. If this requires payment of a deposit, set up a bank account and obtain seed money from the IACR Treasurer.

T−11 Select a local organizing committee (Section 4.3). Refine the budget (Section 5) and approach potential sponsors for your event (Section 6). For RWC sponsorship is vital, and you need to be pro-active in going out, finding, and contacting sponsors. Waiting for them to come to you is not the way to do it.

T−9 Coordinate with the IACR webmaster and the Committee about how to host the symposium website (see Section 7).

T−7 Finalize the budget, set a registration fee, and send the detailed budget to IACR President and Treasurer for immediate review and final approval (Section 5). You must have an approved budget before registration can be opened. To set a low registration fee you should have collected, or be in the process of collecting most of the sponsorship by now; and hence have a good idea of the final figure.

Inquire into obtaining insurance for the event.

T−6 Arrange and announce the registration method. You must use the IACR's own online conference registration system, which also handles credit-card payments and is integrated with the IACR membership database. Since all participants of IACR conferences and symposia are entitled to become members of IACR, using the IACR system ensures that attendee information is recorded in the membership database automatically (Section 8).

The possibility for registering early at a standard fee should be available for at least 2 weeks after the announcement of the final program. The deadline for early registration has typically been about one month before the event; careful choice of this date allows you to plan ahead.

Announce the symposium on the website, to the IACR membership by email, and open the registration (Section 7.1).

If not already done, set up a bank account. Usually if you are based at a university this can be set up within your local finance system at the university.

T−2 Coordinate the schedule with the program chair and the Committee.

T−1 Take care of all major things to organize, like meals, coffee breaks, reception, audio-visual equipment, Internet access (Section 9), but also of minor things, like badges (Section 10).

Be prepared to send Letters of Invitation.

T−2 Monitor registrations through the IACR web interface to intercept fraudulent registrations, manage sponsoring and stipends.

A few weeks prior to the event, you should send an email to all the registered participants with some basic information and a link to the updated website (program, venue, last minute changes).

T−1 At the discretion of the general chair registration fees can be increased at this point in order to encourage people to register early and facilitate your planning. Experience has shown that about 80%–90% of the registrations come in before this deadline.

T The RWC symposium takes place; see Section 11.

T+1 Coordinate with the IACR Membership Secretary and Treasurer for final attendees list, last minute registrations, refunds, address changes, etc.

T+1 Start settling any outstanding financial details.

T+5 Send the financial report and surplus funds to the Treasurer. Take a well-deserved rest.

4 Proposal

This section explains how to prepare a proposal for RWC. Before you start making a detailed proposal, you should contact the Committee. You will get useful feedback on how to proceed and on the deadline to submit your proposal.

4.1 Venue

The choice of a location involves several factors that should be considered early in the process.

Accessibility: RWC draws participants from around the world, and the location should be chosen with this in mind. In the event of a venue located far from an international airport or major train station, convenient and frequent shuttle transportation should be made available. Other important questions are whether IACR members from all countries can attend and whether you anticipate problems with visa.

Meeting facility: The location for lectures should be large enough to comfortably accommodate the expected number of participants. RWC has usually had around 500 participants. It is a clear policy of IACR that everybody who wants to come should be allowed to. On the other hand, a meeting room that is too large will limit the effectiveness of presentations and inhibit interaction. The room (or rooms) used for presentations should have at least one large raised screen. Space for coffee breaks and lunches should be available nearby. Generally meeting rooms at a university are more affordable than at hotels or conference centers.

Consider any transportation problems between lodgings and meeting places.

Lodging: Point out lodging options of different types, ranging from first class (hotel) to one as cheap as possible (student dormitories or equivalent). Ideally, participants should be able to get from lodging to the lectures and back on their own and without much delay, i.e., on foot or at least by public transport that runs frequently. In the latter case, make precise information (also on how to get tickets) available in the map or in the individual hotels.

Cost: Many potential attendees at RWC have severely limited budgets for travel. If the cost of attending the conference is too high, then many people will be unable to attend and the scientific program will suffer as a result. RWC aims to keep registration low by having a very high level of sponsorship. Note, that often it is participants from companies and not academia which have more restricted budgets; especially start-ups which are a key part of the RWC target audience.

For the proposal, investigate costs of lodging, meals, meeting rooms, and local transportation. It is strongly advised that you visit the proposed venue. Also make sure that facilities and lodging will be available at the time desired. Do all of this well in advance and include a set of brochures, photos, fact sheets, etc. together with your proposal.

4.2   Timing

RWC is always in January.

4.3   Organizing committee

Include verbatim Section 3.3 of the IACR General Chair guidelines.

4.4   Format of the proposal

Include verbatim Section 3.4 of the IACR General Chair guidelines. In particular, use the IACR *conference budget planner*.

5   Budget

Include verbatim Section 4 of the IACR General Chair guidelines.

For RWC the budget for student stipends is usually between 20,000 and 40,000 US dollars. This is used to fund hotel and travel for students who would otherwise not be able to attend the event. Priority for this funding goes to students from institutions who have less access to research funds.

6   Sponsors

Sponsoring is *the* major source of income for RWC. Sponsors like to get recognition by having their name attached with an item or to a recognizable part of the program. However, providing an explicit service such as this for sponsorship can count as a "sales" event; and hence can attract VAT in some countries. Sponsorship for RWC is usually treated as a donation to the running of the event; mainly to support student stipends to attend the event. Sponsors should be acknowledged at the event and on the website.

The Committee maintains strong links with sponsors for RWC. To this end the Committee appoints a sponsorship secretary. This secretary is responsible for coordinating requests for sponsorship to the sponsors for previous years. The General Chair is still responsible for finding additional sponsors to reduce the overall costs for attendees. The General Chair and the sponsorship secretary should work closely together in this respect.

7   Publicity

IACR maintains a website at `http://www.iacr.org/`. You can send announcements by email to all IACR members, but you should limit the number of email announcements sent to all members to two for each event.

The primary way for communicating with attendees is online, through the IACR website, the online IACR News system, the RWC website, and other channels (e.g., social media). The first step is to list the event in the IACR calendar of events (members like to know dates well in advance). To do this, fill out a web form at `http://www.iacr.org/events/`.

The RWC website is hosted on the IACR server following a standard template. The Committee will be responsible for sorting out the website.

Once your basic website is set up, make sure that it is linked from the calendar of events and publicize the Call for Contributed Talks. Coordinate with the IACR Webmaster and Communications Secretary to announce the symposium broadly and at the appropriate time.

All communication regarding RWC should clearly state that the meeting is sponsored by IACR by including the phrase "sponsored by the International Association for Cryptologic Research." In addition, you should include the IACR logo (available from the IACR website). If other organizations are helping with the meeting in some way, then you should include the phrases "hosted by" or "in cooperation with" for these organizations, but not "sponsored by."

7.1   Call for participation and other announcements

Include verbatim Section 6.2 of the IACR General Chair guidelines.

8   Registration

Include verbatim Section 7 of the IACR General Chair guidelines.

RWC does not foresee single-day attendance rates nor lower registration fees for people with lesser financial means. The reason being that RWC registration fees are generally quite low. For the same reason RWC has traditionally not allowed refunds apart from exceptional circumstances. The student rate should be half the standard rate.

8.1   Stipends

As mentioned above RWC usually has a generous student stipend pot which is funded by the sponsors. This should be used to waive registration fees and to support lodging and transportation costs for students.

It is recommended that the General Chair process these payments through the local organizing host organization. For example if your "bank account" is a university, then usually a university has a system for processing expense claims for visitors. This should be used to process the payment of student stipends. The reason for this is that different countries have different rules for accounting and tax status of expense claims. In addition, paying stipends directly from the IACR accounts is very complex; and thus this needs to be processed locally.

8.2   Integration into IACR membership

Include verbatim Section 7.7 of the IACR General Chair guidelines.

8.3   Registration confirmation

Include verbatim Section 7.8 of the IACR General Chair guidelines.

9   Major Things to Plan

Include verbatim Section 8 of the IACR General Chair guidelines, with the exclusion of Section 8.5 (proceedings) and 8.6 (excursion).

Note that RWC does not normally provide any evening meals nor rump session, and that lunches are usually "light" sandwich-based lunches. This is to keep registration costs down. Sometimes a small drinks reception on the first day (or on the evening before) is organized.

10   Minor things to plan

Include verbatim Section 9 of the IACR General Chair guidelines. Exceptions: RWC does not usually have a souvenir nor a photo to reduce cost; the list of attendees is available online to registered participants.

11   At the event

Include verbatim Section 10 of the IACR General Chair guidelines,

12   Financial guidelines

Include verbatim Section 12 of the IACR General Chair guidelines.

13   Preparing the program

This section is aimed at the Committee and the program committee for a given year.

The RWC symposium lasts for three days and consists of talks; about half of which are invited and half of which are contributed. About half the talks should be from industry and about half from the "applied" side of academia. The primary selection criteria are that the talks should be of interest to the audience, and that the speaker should be able to give a good exposition of their material.

The invited talks are invited by the RWC Steering Committee, and are usually either about interesting topics which have occurred during the year, or from people in industry who the committee think have something interesting to say.

Contributed talks are "light-touch" reviewed by a separate program committee consisting of six invited reviewers, plus six members of the RWC Steering Committee. The chair of the program committee is appointed by the RWC Steering Committee. Usually potential contributed talks are solicited via a "Call for Contributions" (the IACR *websubrev* system could be used for this). The "paper" being a short outline (1-2 pages) of what the talk will be about. The role of the program committee is to select the best such proposals, bearing in mind the need to maintain a balanced and interesting program.

Strong academic research results have other venues (IACR General Conferences and Area Conferences) and product descriptions also have other venues (RSA Conference etc). Thus talks are selected primarily on the basis of whether the speaker is going to give a good talk on something which the audience will find interesting.

One can sensibly fit in around six hours of talks per full day, assuming lengthy coffee and lunch breaks to facilitate discussions. Thus one expects at most 36 half hour talks over three days. Hence, the goal is to obtain *at most* 18 contributed talks and *at most* 18 invited talks. Some talks will be given a little longer than half an hour if the committee feel it is needed.

14   Levchin Prize

Two Levchin prizes are awarded each year. These are prizes in the area of real-world cryptography, which have been kindly supported by Max Levchin. Who receives these awards is at the sole discretion of the RWC Steering Committee.

15   More information

More information is available on the IACR website at `http://www.iacr.org/`; browse the website and obtain information about past conferences and workshops. Do not hesitate to contact the members of the Committee and the Board for more information.

The current Committee is listed on the RWC website at `https://rwc.iacr.org/`.

The current Board is listed on the IACR website at `http://www.iacr.org/bod.html`.