# IACR Policy for Cryptology Schools

August 2016*

## 1 Purpose

In 2013, the IACR has discussed a new move to allocate support for *Cryptology Schools*; typically these are educational "summer" or "winter schools" aimed at graduate students. The IACR selects proposals for Cryptology Schools, gives organizational guidance, and provides financial support, but does not assume financial responsibility for the event organization.

This document briefly recalls the rationale behind this action and presents the guidelines for implementing Cryptology Schools. It describes the Schools Committee, the selection procedure, and directions on how to run a school.

## 2 Overview

**Goal.** In the tradition of academic "summer and winter schools", a Cryptology School provides intensive training on a clearly identified topic in cryptology. Its aim is to develop awareness and increased capacity for research in cryptology. Sometimes, particular focus may be given to regions where cryptography research and education is under-represented, even though excellent local potential may exist. For instance, at the time of writing (2014), Eastern Europe is one such region — despite a highly motivated population of students and researchers with strong mathematical background, the lack of local resources has led to insufficient exposure to the approach of modern cryptography. The region is currently not adequately represented at the forefront of research in modern cryptology.

Moreover, also at some institutions with a long tradition in cryptologic research, the local expertise may not cover all aspects of the field and can be focused on a few topics only. This means that students get a narrower view of the field than what is desirable. Organizing a Cryptology School at such institutions can be a cost-effective way to expose students to a broader range of topics presented by top experts.

**Format.** A Cryptology School is typically held full-time for 4–5 days of intensive learning and constitutes an efficient way to provide high-quality training for graduate students, as well as for professionals. Attendance should be open to anyone who is interested and qualified (at some popular schools, attending students may be asked to submit a letter of recommendation by their supervisors or attendees may need to solve a puzzle before they are eligible to participate).

*The most recent version of this document can be obtained from `http://www.iacr.org/docs/`.
Editors of this document: M. Abdalla, A. Boldyreva, C. Cachin, A. Kiayias, B. Warinschi (2014).

In order to facilitate learning, a school is usually taught by a few domain experts with a focus on educating the audience rather than impressing with results. In line with the mission of IACR, a Cryptology School should enable the audience to advance the theory and practice of cryptology and related fields. At some schools graduate students may also get an opportunity to present their work and gather feedback from the experts and teachers.

## 3 Schools Committee

Support for a Cryptology School is approved by the Board of Directors upon the recommendation of a *Schools Committee*. The Schools Committee is responsible for the implementation of the IACR policy for Cryptology Schools according to this document.

The Schools Committee consists of 5 members; its chair must be a member of the Board and it is desired that at least one other member of the Schools Committee is also a member of the Board.

The Schools Committee is appointed by the Board of Directors at the beginning of every calendar year, on the basis of a recommendation of candidates made by the Schools Committee of the past year. It is suggested that at least one of its members changes each year.

## 4 Selection Procedure

Proposals are selected by the Schools Committee and approved by the Board of Directors. An application for Cryptology School should follow the procedure described here.

**Proposal Format.** A proposal for a Cryptology School should provide the following information in a clearly marked structure.

1. Name and topic of the school. This section should include a short description of the topic of the school and provide an explanation of how the topic is relevant and timely for cryptology research.

2. Objective. The section should explain the goals of the school and the expected benefits for the participants upon the school's completion. It should be clearly indicated what kind of skills or knowledge will be imparted to the participants and what are the requirements of the participants prior to the beginning of the school. It should also be indicated what kind of materials will be made available to the participants (notes, slides etc.).

3. Estimated number of attendees.

4. Location, time, and accessibility. Items for this section include description of travel options and accessibility during the particular time of the year of interest, details about local commuting if the school is in a remote location or the housing is separate from the conference hall, details about housing facilities and the conference room arrangements.

5. Potential speakers. It is important to indicate what subset of speakers have already committed or "soft-committed" to participate and give lectures at the event.

6. Format for all the talks (time, slots).

7. Budget. A sufficiently detailed budget should be given, including full information about funding sources other than the IACR. Is there a risk of running a deficit and who would absorb it? No profit should arise from the school. It is important to note that IACR will only provide partial or "seed" funding for the school and does not assume financial responsibility. Therefore, it is vital that organizers secure other types of funding or ensure that participants can pay for their participation themselves. Note that if a registration fee is charged then that fee must comply with the IACR's non-discriminatory policy on registration fees (see IACR Guidelines for General Chairs, Section 7.5).

In general, to minimize the risk and to simplify the cost model, the IACR intends to sponsor mainly fixed costs (event location, travel for speakers, etc.); the participants or other sources would absorb the variable cost (lodging, food, and any other per-participant cost). This model has proved effective for schools organized by the EU-FP7 ECRYPT projects. Speakers should generally be reimbursed for their direct costs, but no honorariums must be paid. Receipts should be collected for demonstrating how the IACR funding has been used.

**Deadlines.** There are two rounds of submissions every year. The submission deadlines are:

- *December 31st of year $X-1$:* For schools that take place between May of year $X$ and April of year $X+1$.
- *June 30th of year $X$:* For schools that take place between November of year $X$ and October of year $X+1$.

**Evaluation.** The Schools Committee selects a number of proposals within one month after the submission deadline and forwards them with a ranking to the Board of Directors. The Board decides on approval of the selected schools within one month after receiving the proposals from the Schools Committee.

The amount allocated per deadline will depend on the number and the quality of the submissions. Specifically, the Schools Committee will review all submissions and will decide to fund proposals according to the following criteria:

1. Relevance of the topic and commitment to further research in cryptology and related fields;
2. Potential for high impact in both education and research;
3. Quality of speakers and credibility of the organizers; and
4. Convincing and feasible organizational plan.

Schools that have received previous IACR funding may receive lower priority for repeat funding.

## 5 Organization of a School

The Schools Committee informs the organizers about the selection and maintains contact with the organizers. The organizers commit to follow the policy for Cryptology Schools according to this document.

After approval, the organizers of the school may use the name *[IACR] Cryptology School* for advertising the event. They should include the school in the IACR Calendar of Events in Cryptology on the IACR website and coordinate further publicity actions with the IACR Communications Secretary and/or webmaster (`webmaster@iacr.org`).

The organizers are responsible for handling registrations, organizing the venue, collecting fees, and so on. The IACR sends its contribution to the organizers as a lump sum; the organizers take care of the direct reimbursement of costs. The organizers should prepare written justification, such as receipts, for all incurred expenses covered from IACR funding. Unused funding from the IACR must be returned.

## 6 School Report

After completing the school, the organizers are responsible for providing to the IACR *two reports* about their event.

1. A public summary of the event, giving sufficient details about the talks, the number of attendees, the program, and any other noteworthy aspects of the school. This summary will be published on the IACR website.

2. A financial summary of the event that indicates how the support of the IACR has been used and includes the corresponding receipts. This report should be sent to the Schools Committee and will not be circulated beyond the Board.

These two reports must be received within 1–2 months after the school.