A More Detailed Strawman for Proceedings of the IACR

N.P. Smart,
Incorporating ideas from
Alex Dent, Phong Nguyen, Hilarie Orman,
Martijn Stam, and Christopher Wolf.
Thanks for Kevin McCurley for data for 2012

IACR—International Association for Cryptologic Research

1 Motivation

Every year, the IACR is currently running three major *conferences* (Crypto, Eurocrypt, Asiacrypt) and four *workshops* (CHES, FSE, PKC, TCC) focused on particular topics. In total, the yearly submission count is about 1189, and the total amount of accepted papers is 256 (figures from 2012, see Section 4) which gives an average acceptance rate of 21.5%. So even *without* taking the Journal of Cryptology into the game, the IACR is running a serious submission/reviewing business that needs looking after itself from time to time.

The proposals in this document aim to review the procedures and suggests some major modifications. The main "headline" options are derived from various options which the IACR Board of Directors (BoD) has considered and are known to be achievable with various publishers. After detailing the deadline options, this document then goes on to elaborate on an implementation plan for one of the options. The reason for doing so is *not* to pre-suppose any decision, but to explain to members the kind of knock on consequences which may follow from a given decision.

Before proceeding it is perhaps worth outlining some Major and Minor goals that we would like to achieve.

1.1 Major Goals

1. Move to a fully open access method of publication. This needs little explanation, and is the desired wish of the members as demonstrated at many member meetings.
2. Referee and publish full papers. Thus removing the multiple version of a paper problem and improve overall quality of our output. Internally our community refers almost always to the full version of papers in the eprint archive, but the article of record is nearly always the shorter conference version (14-20 pages). Such a situation is hard to explain to external people (funding agencies), and hard to justify scientifically.
3. Acknowledge we do multi-round refereeing (currently called sequential submission to conferences), but do it in a more cost/time efficient manner for the referees. PC members who serve on many committees see as many as 25 to 30 percent of papers in their pile coming from previous meetings. Multi-round reviewing is seen as a quality mark in most other non-CS areas. If we do it, we might as well get credit for it, and do it in a more efficient manner.
4. Move to a journal system to improve external credibility. Many in our community need to continually explain to both funders and senior managers that publication is via conference presentation as opposed to journal publication[1]. This makes it very difficult to comply often with funders or managerial requirements re funding.
5. Decouple the conference presentation from the publication process. This could enable us to be indexed fully by ISI. ISI does not fully index conference proceedings or journals that act like conference proceedings: citations in such publications to 'proper' journals are counted, but no quality rating (impact factor) is produced. Full ISI indexing and impact factors are important politically in many countries; it also enables us to use a rigorous citation methodology used in other areas of science, as opposed to relying on dedicated web-search engines, such as Google Scholar. It is also important to note that it takes at least three years before ISI assigns an impact factor.

[1] The historic motivation to chose for conferences was speed of publication.

1.2 Minor Goals

1. Remove deadline rush.
2. Shorten the overall time that a paper spends in review.
3. Deal with bandwidth limitations.
4. Simplify the publication model and the supporting infrastructure (by removing multiple version problem).

2 Options

We now outline four possible options, which we reiterate can be accommodated with various publishers:

2.1 Option A:

Stay as we are with Springer LNCS using the current per-conference committee approach. In this case we cannot meet Major goals 3, 4, and 5. Major Goal 1 can be met at very large cost to the authors and/or IACR, and Major Goal 2 could be met by increasing the size of each LNCS volume to about 2000 pages (3 volumes) for a flagship conference.

2.2 Option B:

Move to a USENIX/STACS-style model, where IACR acts as publisher. In this case an ISBN number is assigned and ISI would still index the papers as conference papers. Publication means that a paper appears on the IACR publication site and on some public archives; paper volumes could be printed on demand. Here we can easily meet Major Goals 1 and 2. But Major Goals 3, 4 and 5 are again problematic. There is also the issue as to whether the USENIX/STACS-style publication model is acceptable in the community.

2.3 Option C:

Keep the IACR workshops with LNCS, and move the conferences to a journal based system. This is a limited form of Option D below. With this option we can achieve Major Goals 1 and 2 within a reasonable cost; Major Goals 3, 4, and 5 will be only partially met as the workshops will be excluded.

2.4 Option D:

Move all IACR workshops and conferences into a journal based system. This *could* meet all Major Goals and it is the option which is worked out below. Options C and D are inspired by the model adopted for the "Proceedings of the VLDB Endowment" (see `http://vldb.org/pvldb/`).

3 Timeline

If any change is going to be implemented in time for the next contract negotiation then the lead time is quite long. We really need a decision to be in place by Dec 2014. Thus the following timeline is suggested:

- July 2013: Distribute this document to members.
- August 2013: Discuss at CRYPTO.
- Oct 2013: Filter any changes and update.
- Dec 2013: Discuss at ASIACRYPT.
- Dec 2013: Steering committees of CHES, FSE, PKC and TCC decide whether agree in principle by end of year.
- March 2014: Final draft of proposal.
- May 2014: Present final proposal at EUROCRYPT.

– Oct 2014: Vote by members on approval of the Option (A, B, C or D)
– Q1 2016: Complete IT system that can deal with the new model.
– Q1 2016: Complete negotiation with publishers.

At this stage we are only discussing the general option. But to ground this in something concrete we give details below of Option D (being the most radical) outlined in some detail. These details are not set in stone, and once the specific option is selected a group will need to be convened to work out the details.

4 Statistics

Before proceeding it is good to look at the scale of our operation. In 2012 we had the following figures for each conference accepted/submissions:

Conference	Asiacrypt	Crypto	Eurocrypt	CHES	FSE	PKC	TCC
Accepted/Submitted	43/241	48/225	32/195	32/120	24/89	41/188	36/131
Percentage	17.8%	32.3%	16.4%	26.7%	27.0%	21.8%	25.5%

This gives a total number of 256 accepted papers and a total number of 986 submitted papers (including sequential double submissions); giving an average acceptance rate of 26 percent. The total number of people serving on program committees in 2012 was 170 (see the Appendix for the list obtained from CryptoDB). If a reader of this document does not recognize names in this list, note it represents the entire field of cryptology and shows the diversity of our community.

However, things are a bit more complicated. In particular, over the years, the number of submissions have gone up while the number of abvailable slots has stayed virtually constant over the years. Lars Knudsen has a very complete dataset on this[2]. For example, take the submission/acceptance rate at Crpyto. Here we have

	Crypto 1990	Crypto 1995	Crypto 2000	Crypto 2005	Crypto 2010
Accepted/Submitted	42/104	36/151	32/120	33/180	39/202
Percentage	40.8%	23.8%	26.7%	18.3%	19.3%

So in total, the acceptance rate has gone down while the number of submissions was on the rise. Or to rephrase this: To keep the quality at the same level as in 1990, the number of *accepted* papers would need to double. As the number of slots of a conference is limited, this leads to a "bandwidth problem" in that the field produces overall many more papers than what can be published. Whilst this in some sense links "quality" and "quantity", we can see the breadth of the field increasing (the introduction of the workshops), as well the as the number in the field increasing (the number of members).

In addition, there is the problem of "cycling" papers that are being submitted to one conference or workshop after another (with only small modifications) – until they are finally accepted at a given desired venue. In a sense, these cycling papers complicate the review process, as they require review attention from each single programme committee. In the experience of some PC members who serve on a large number of committees (Nigel Smart), the fraction of these papers can be as large as 30 percent. Unless these papers are seen by the same reviewers, this means another set of referees are reviewing "from cold" each time. This increases reviewer load and should be compared to what happens in journal submissions.

5 Details for Option D

Let us assume for the moment that we assume we have the conferences and workshops included in a journal model; which for now we will call the Proceedings of the IACR, a.k.a. Proc. IACR. This can easily be changed to just the conferences; but working out the details for the maximum case is the harder case. In what follows in this document, we therefore assume the total number of *distinct* papers is around 800 per year, which

[2] `http://www2.mat.dtu.dk/people/Lars.R.Knudsen/accrates.html`

works out at 15 papers per week or 67 papers per month. Which works out as an overall acceptance rate of around 30 percent if we assume there are only 800 real individual submissions per year.

Moving to a journal model will allow us to publish full papers (Major Goal 2), will enable simplified multi-stage reviewing (Major Goal 3), and immediately hit Major Goal 4. We are confident that we can obtain a deal that is financially acceptable for open access with a reputable publisher (Major Goal 1) due to prior work during the previous contract negotiation[3]. So as to decouple conference presentation from the publication process (and Major Goal 5 after 3 years, that is, in 2020), we organize the process into two stages.

1. The Proceedings of the IACR assess the quality of papers and allow for speedy publication
2. All IACR workshops and conferences can draw from this pool. These committee for programme selection can be smaller and more effective than before as they do not work on papers, but on the output of the reviews of papers.

We could even extend the model to include other workshops as need be.

5.1 Honour Code

We need an honour code to ensure things work. The process relies on authors and referees not trying to game the system. Thus we need to penalise people who abuse the system. This is not different from what most journals have today.

So for example authors who submit clearly incomplete or rushed papers will have their papers immediately rejected, with possibly (at the discretion of the editorial board) no resubmission for a full 12 months.

On the other hand referees who do not fully referee papers, or submit tiny reviews will be noted and not invited back. Given senior people use editorial duties as an indicator of excellence this is not in their interest to exclude themselves from refereeing. This in some sense already happens in journals, and to some extent in conference PC selection.

As with all "games" there needs to be a referee; this will be in the Editor in Chief (see below), who is ultimately responsible for all decisions. Since the EiC reports to the BoD, and the BoD is elected by the members of the IACR this provides accountability. In addition the ethics committee will have oversight of the procedures and advise both the EiC and the BoD of any issues. In addition there should be a mechanism for authors to complain about summary rejections, insufficient or rude reviews, etc. Without the time deadline of a conference to organize such issues can be dealt with calmly and in a better way in future.

5.2 Management

In this section we propose a possible management structure.

The entire procedure will be coordinated/managed by a single *Editor in Chief* (EiC), who will be appointed for a period of three years by the BoD (much like the EiC of the Journal of Cryptology). They will have a position on the BoD (much like the EiC of the Journal of Cryptology), and will be appointed in roughly the same manner. The roll of the EiC is to ensure the procedures are followed and that the Editors (see below) follow the procedures correctly and in a timely manner. They will also resolve any conflicts or disputes and report on the operation to the BoD.

Below the EiC will be ten Editors. These could be appointed as follows:

- The Board of Directors (BoD)[4] of the IACR will appoint three persons each year; one from each geographic area of Europe/Israel, the Americas, Rest of World. Each of these persons will server for a period of two years. The pairs of representatives will act as the chairs of the programme subcommittees for Asiacrypt, Crypto and Eurocrypt. This mimics the current six co-chairs of Asiacrypt, Crypto and Eurocrypt. It ensures our diversity of geography is maintained.

[3] The cost would be 300-500 US$ per paper, which is comparable to the pre-2013 scheme but more expensive than the 2013-2016 Springer contract.

[4] As per the current procedure for programme chairs this will be done by the elected members only

– The four steering committees will each appoint one person each year to represent the four workshops of CHES, FSE, PKC and TCC. The term of each of these people will last for one year only. To mimic the PC chairs of the current workshops. To also make sure our diversity of subcommunities are represented.

These ten Editors will be in place before September in year X-1, giving them four months to select Associate Editors (see below) for year X.

The ten editors will appoint roughly 155 distinct associate editors in total; each one serves for one year. We expect each associate editor to organize the reviewing of up to 20 papers per year. If a papers reviewing passes over the term of an associate editor then the associate editor is retained purely to ensure the continueing refereeing of the papers.

– If we have 800 papers to review, each needing three reviewers and each associate editor is only going to deal with 20 papers per year, then we need 120 associate editors. With each associated editor only dealing with 20 papers over one year, this means a significant reduction in reviewing for people who serve on multiple committees in the current structure. However, by going to 155 associate editors we are actually using less editors than the current system. Yet with 155 associate editors we can perhaps reduce average reviewing of papers per person. However, we are now also refereeing more pages, so the two can balance out somewhat.

Associate editors can be appointed for further years if the editors wish this; indeed given the size of the community it is highly likely that associate editors will be selected year on year. In addition, appointment of associate editors as the year progress to adjust for varying workload etc. will be encouraged. The aim should be to however appoint 155 before the year starts.

The editors will appoint associate editors on the basis of producing the best coverage of expertise for the papers being expected; with no account being taken of geographic location (i.e. the equivalent of the Crypto PC chair does not just select people from the Americas). The editors will appoint the associate editors in the following order:

– The CHES, FSE, PKC, TCC steering committee-appointed editors will each appoint 20 associate editors first to ensure coverage of their technical areas. This ensures that the overall set of associate editors is diverse in area.
– Then the three pairs of BoD-appointed editors (now known as Asiacrypt, Crypto and Eurocrypt PC chairs) will appoint a further 25 associate editors for each pair. This gives an additional 75 associate editors in total. This can be done in any manner; but given these chairs are more senior generally one suspects this will be amicable; and a number of people they would have selected have already been chosen already in the first step.

When selecting associate editors, the editors should ensure that a reasonable number of new faces are introduced each year to avoid the community ossifying. In doing so we aim for 10 percent of all associate editors each year to have served for less than 5 other years (or equivalently 5 conferences/workshops during the initial few years). One of the EiC's role is to ensure this happens; by liasing with the IACR Secretary who currently maintains a list of good junior people who have not been selected to be on PCs.

On appointment each associate editor agrees to referee 20 papers over a period of 12 months. As we expect papers to come in over the entire year the associate editors will have the option of marking two months of the year as being "unavailable". Associate editors which refuse to deal with papers and which have not dealt with 20 in the year (without a genuine reason) will be recorded for future editors information. A similar recording will be performed if an editor feels that an associate editor has not returned reports which are acceptable. After all if we are asking authors not to submit rubbish, we need to ensure referees also agree to the same. The EiC will be responsible for recording this information, so as to maintain a corporate memory.

5.3 Paper Submission/Author Actions

Papers can be submitted at any time. A paper submitted is assumed to be a full paper; and referees are expected to read them entirely. Of course an author could say that a proof is not included, but a referee can then say "reject," as a proof is not included. Thus production of "extended abstracts" is discouraged.

When submitted an author *can* mark one (or more if it makes sense) of the following categories:

- CHES (I would like this paper considered for publication at CHES).
- FSE (I would like this paper considered for publication at FSE).
- PKC (I would like this paper considered for publication at PKC).
- TCC (I would like this paper considered for publication at TCC).
- No Talk (I do not want to present this at ANY workshop *or* conference).

A workshop editor can at their own discretion add a tick to any paper; just to ensure relevant papers are considered for the workshops.

An alternative method would be for the authors to be given the same choice *after* there paper has been accepted and they know their overall grade. They can then take into account the choice given their geographic preferences for the upcoming meetings. Although if relevant PC committee can still decline to take their presentation.

We guarantee a response to the author in the following (rough) time scales:

- 30 Pages or Less: Two Months
- 45 Pages or Less: Three Months
- 60 Pages or Less: Four Months
- 61 Pages or More: Paper is transferred to Journal of Cryptology process.

This time line is indicative so there is no point in authors trying to cram a 40 page paper into 30 pages (presumably a page and font size/type would be defined).

Papers can be returned with one of three codes (Accept, Reject, Rework). At the discretion of the editor dealing with the paper a rejected paper cannot be resubmitted for a period of one calendar year, even with changes. The editors can also ask for a resubmission earlier than one year if this is deemed appropriate. If an author ignores a request to not to resubmit they will be referred to the ethics committee; who could impose various penalties on the author.

A paper asked for Reworking can be resubmitted together with an author response; this must be done within *one month* after the initial notification. If no response is received within one month *and no extension is granted by the corresponding editor* then the paper is deemed to be withdrawn (which can be treated like a Reject as above in terms of resubmission). A reworking *must* address the concerns of the reviewers, either by arguing against the referees conclusions, or by incorporating the changes required. A letter detailing the response must be submitted with the resubmission.

On resubmission of a paper asked for reworking, a paper will be returned into the discussion phase (see below), and a response (again Accept, Reject, Rework) will be returned within half the time of the initial review (so one month for 30-page papers, 1.5 months for 45-page papers, 2 months for 60-page papers). This process may carry on one more time, for a maximum of three submitted versions (the initial submission and two revisions). Thus the maximum time a 30-page paper can last in the system is six months (two months initial review, one month for first revision and author response, one month re-review, one month for second revision and author response, one month final re-review).

5.4 The Review Process

The editors on receiving a paper can decide to instantly reject it for one of the following reasons

- Out of scope
- Poor presentation
- Clearly too weak for selection

We expect about 10-20% of all papers to be rejected in this manner. This will reduce the reviewing load and these percentages seem to be consistent with some of the papers we get. Papers longer than 61 pages are instantly redirected to the Journal of Cryptology. Any paper which does not meet the submission guidelines (in terms of formatting etc.) should be instantly rejected. Any such instant rejection must be agreed upon by two editors.

Within one week the editors will assign an incoming paper to three associate editors. The associate editors are then charged with obtaining a *full* review in the following time scales:

- 30 Pages or Less: One Month
- 45 Pages or Less: Two Months
- 60 Pages or Less: Three Months

The reviewing software will be tweaked to enable the efficient management of these timelines. There will be no extra reviewers for associate editors papers; since essentially everyone who is anyone is an associate editor. This last point should be compared to current system of five reviews for PC member papers; the recent tendency for large PC's results in this adding to the reviewing burden.

After the initial three reviews the paper enters a one-month discussion phase.

For example, the first two weeks of every month are reserved for discussion; with the second two weeks for making a decision on the paper.

This is open to all associate editors (bar those who have a conflict of interest with the paper). The editors need to encourage associated editors to help in the discussion. The goal being to come to an Reject, Accept, Rework decision; with a clear definition of what reworking is needed. Note, the goal is to accept about 30 percent of all papers submitted. This could be slightly more as we may not have all papers presented at each conference.

- The 30 percent goal here is based on current standards, and current volumes. Clearly an acceptance criteria is based on a quality threshold and not on numbers. As the community increases/shrinks this percentage may change. But in the initial run we should expect a 30 percent acceptance rate.

In other words the standard for the Proceedings of the IACR will be at about the same level as the current standard for the workshops.

When a paper returns into the discussion phase after reworking, an additional associate editor is assigned to it; and again for the second return into the discussion phase. The new associate editors should check the authors have responded to the reviewers initial queries. They also need to ensure that the referees are not being overly harsh with a paper and are not acting in an adversarial manner. Thus when a paper is rejected after a second discussion phase an author is assured that five associate editors have been heavily involved in the decision.

When a paper moves to reject as a quick sanity check, for any paper which is marked as suitable for a workshop the editor associated to that workshop needs to approve of the reject. We have a tendency to be negative towards certain sub-areas; e.g. FSE/CHES like papers. Indeed referees in this area are usually more aggressive towards their own style of papers than other sub-areas. By installing a check this means we will not reject all FSE/CHES papers (say) and so leave none to present at the workshops.

5.5 After Acceptance

After acceptance a paper is passed to the Proc. IACR for publication as soon as possible. This needs to be very fast, and hence a good contract needs to ensure this happens.

Up to this point we have not really talked about conference presentation. And this is deliberate; we want to decouple conference presentation with paper refereeing and publication.

Suppose a conference/workshop occurs in month Y, then in month $Y-4$ the editor convenes a virtual PC (of around 20 people). The PC takes the set of papers currently accepted (on a specific date, so no new papers are added in to confuse things), and picks a subset to be presented at the conference.

The PC of a workshop or conference can decide to run their conference anyway they want (20 min talks, 45 min talks, parallel sessions or whatever). As each paper is selected an invite is sent to the author (i.e. not all in one go). Once selected an author (or set of co-authors) is informed and they have two weeks to respond to say whether they accept the invitation to present their accepted paper at the meeting. They can decline.

For the conferences the PC's job is to ensure an excellent program which spans *all* areas of the subject. Our flagship conferences are meant to represent the entire community and bring everyone together. For the workshops they should take into account the preferences selected by the authors above.

After one year[5] from acceptance an accepted paper is removed from the list of papers for possible presentation. Thus a paper may not be accepted for presentation; and in addition an author may decline presenting at one meeting (with a view to getting an invite later) and the expected second invite never materializes.

An example is perhaps illustrative. Suppose we have the following calender: Jan(-), Feb (TCC), March (PKC), April (FSE), May (Eurocrypt), June (-), July (-), August (Crypto), Sept (CHES), Oct (-), Nov (-), Dec (Asiacrypt).

Now suppose a paper reaches the accept state in late August in year X and is marked as a paper which says thinks would be suitable for PKC and the author is based in Western Europe.

- The paper misses the consideration for Asiacrypt (deadline 1st August) for year X.
- The next time it will be up for consideration is for PKC at the Nov cutoff (it is not considered for TCC, as the authors did not tick this option).
- It is offered a speaking slot at PKC, but the author declines as they want to really present at Eurocrypt or Crypto.
- The paper returns to the pool, and is considered for publication at Eurocrypt (decision in Jan year $X+1$) and Crypto (decision in May year $X+1$).
- However, the PC subcommittee for these conferences does not accept the paper.
- Now the paper is still eligible for Asiacrypt, since it was not accepted in time for Asiacrypt the year before.
- The paper is offered a speaking slot, but since Asiacrypt is in Easter Island that year the author has to decline the offer due to the cost of travel.

Thus the paper passes into history, it is published but not presented; but in some sense this was the authors choice they were offered two speaking slots.

5.6 The Role of Editors/PC Chairs

The current proposal essentially defines two tasks of the "Editors". Firstly to act as an editor of a journal, and secondly to act as a PC Chair for a conference or workshop. The basic idea is that these are seperate roles and essentially independent. Indeed we could appoint different people to do the different roles.

- September 2019 – Anna is appointed PKC Editor
- January 2020 – Anna's associate editors start processing papers, with Anna chasing them down.
- January 2020 – Anna starts selecting a program for PKC 2020 from papers accepted in the prior year.
- April 2020 – PKC 2020 is held
- Dec/Jan 2021 – Bob takes over from Anna
- Jan 2021 – Bob starts selecting a programme from papers processed by Anna and her cohort (plus perhaps a few older papers).
- April 2021 – PKC 2021 is held

It could be more rewarding for people if they have responsibility for the program they put most work in. One could of course say that Program Chair is a different role from Editor, or that there is some sort of co-chair model where the past Editor is brought back? Due to the proposed calendar-year terms, the Eurocrypt experience (where you start your term with program selection) will also be quite different form the Asiacrypt

[5] This is not a calendar year, but a conference cycle year since the conference/workshops can move within a year. Basically each paper is "eligible" (in theory, but clearly not in practice as few CHES like papers are eligible for TCC and vice versa) for seven venues on acceptance.

one (where you cap of your term with a conference). Indeed this is true and there is something to be said for having editors start 14 months before their conference/workshop.

The proposal above is however done to ensure the simplest implementation. By selecting on calendar years it is easier for the EiC to ensure that, in calendar year X, the editors have done there job in time of selecting a PC. In addition this means all associate editors are selected at the same time, making the editors roles easier.

Both models re timing have pros and cons.

6 Role of Journal of Cryptology

We want to protect JoC, and run it alongside the Proceedings. Other learned societies have multiple journals and outlets. For example: American Math Society has the Journal of the AMS, Proceedings of the AMS, Transactions of the AMS and Bulletin of the AMS; plus a number of others. The London Math Society also has Journal of the LMS, Proceedings of the LMS, Transactions of the LMS and Bulletin of the LMS; plus a few others.

We already have said that longer papers are sent directly to the journal. In addition to encourage papers to be submitted to the journal we could also have that we replace one invited talk at Asiacrypt, Crypto and Eurocrypt each by having it being given by the top three papers in the Journal in the last twelve months.

Another role is that we are lax as a community in having survey papers, or historical overviews. For example nearly ten years after the first attacks on hash functions we have no single comprehensive treatment of how the techniques work etc in an accessible format for researchers. We could encourage, maybe commission, such surveys for the journal.

7 Relation to Other Events

There certainly is a point that the IACR should take care about its own 7 venues (Crypto, Asiacrypt, Eurocrypt, CHES, FSE, PKC, TCC) first. Even if we *only* integrate these 7 into one big reviewing system —hence ensuring the same quality for all our publications and reviews— this will be huge enterprise. Consequently, extending the scope of this proposal beyond these 7 venues will make the task more difficult. However, as the IACR aims to promote cryptologic research as a whole (from our bylaws), we have a responsibility to maintain variety in our workshop culture.

We could establish a mechanism similar to the current "events in cooperation with" (ICW), where the editors (not associate editors!) allow another workshop (similar rank as our own four workshops) to become a "presenting venue". If this status is granted, the corresponding workshop participates in the "paper bidding" (see Section 5.5) as our own workshops. Given that all these venues have their own scientific value, authors will choose wisely where they want to present. As ICW, the status should be given on a year-by-year basis. One factor could be the number of authors that *accept* presenting at this venue. If the number becomes too small, this is obviously an indicator, that the corresponding venue is of too low quality of the IACR Proceedings.

Moreover, if we decouple the editors and associate editors from the program committees, we have no theoretical limit on the number of workshops we can incorporate.

8 F.A.Q.

Why include the Workshops in this plan? Why not focus on the conferences only?

If we only did the conferences this would not solve the problem of refereeing full papers for the workshops, it would also not solve the multiple refereeing problem (since papers rejected from a conference would then be referee'd again when submitted to the workshops).

Will this not mean that the conference quality will be diluted to that of the workshops?

No, since the conference chairs and their committee still pick the papers they want and the authors can try to play their luck with papers they think are good by refusing to present at the workshops.

What about author anonymity?

The community is roughly split about whether we should have author anonymity. Without reiterating the arguments a brief summary is as follows: From one side "referees if they know a top person wrote a paper do not have to spend so long looking at it", whereas the other side says "Exactly, referees should not be influenced by who an author is, they should read and check everything". In the new system since there are less time pressures and *all* papers are refereed, this question can be revisited.

How to deal with paper choices for workshops/conferences at the same time?

What if PKC and Eurocrypt were both held in the same month? They would be selecting papers in the same month which could be a problem. Hopefully the relevant PCs would talk to each other to ensure that both programmes were successful in this case.

A Program Committee Members of IACR Conferences in 2012

A Tria, Adam O'Neill, Aggelos Kiayias, Akashi Satoh, Alex Biryukov, Alexander May, Alexandra Boldyreva, Alon Rosen, Amit Sahai, Amos Beimel, Anne Canteaut, Antoine Joux, Ari Juels, Arjen K. Lenstra, Axel Poschmann, B Örs, Bart Preneel, Benedikt Gierlichs, Benny Applebaum, Benoit Libert, Berry Schoenmakers, Carles Padro, Catherine H. Gebotys, Cedric Fournet, Chris Peikert, Christian Rechberger, Christiane Peters, Christophe Giraud, Colin Boyd, Colin D. Walter, Dai Watanabe, Dai Yamamoto, Damien Stehle, Dan Boneh, Daniel J. Bernstein, Daniel Wichs, Daniele Micciancio, Dario Catalano, David Cash, David Pointcheval, Dennis Hofheinz, Dipanwita Roy Chowdhury, Dmitry Khovratovich, Dominique Schroder, Dominique Unruh, Dong Hoon Lee, Dongdai Lin, Dov Gordon, Duncan S. Wong, Eike Kiltz, Elisabeth Oswald, Emmanuel Prouff, Eran Tromer, Erkay Savas, Feng Bao, Florian Mendel, Franois-Xavier Standaert, Georg Fuchsbauer, Gil Segev, Gilles Van Assche, Gregor Leander, Guang Gong, Guido Bertoni, H Drexler, Henri Gilbert, Hongjun Wu, Hugo Krawczyk, Iftach Haitner, Igor E. Shparlinski, Ivan Damgard, Ivan Visconti, Jean-Sebastien Coron, Jens Groth, Jesper Buus Nielsen, Joan Daemen, John Black, John Kelsey, Jonathan Katz, Jorn-Marc Schmidt, Juan A. Garay, Jung Hee Cheon, Jurg Wullschleger, Kaisa Nyberg, Kaoru Kurosawa, Kazue Sako, Kenneth G. Paterson, Kenny Paterson, Kerstin Lemke-Rust, Kris Gaj, Krzysztof Pietrzak, Lars R. Knudsen, Leonid Reyzin, Louis Goubin, Marc Fischlin, Marc Joye, Maria Naya-Plasencia, Martijn Stam, Martin Hell, Martin Hirt, Masayuki Abe, Matthew Green, Matthew J. B. Robshaw, Matthieu Rivain, Michel Abdalla, Mike Rosulek, Miroslaw Kutylowski, Mitsuru Matsui, Moti Yung, Nachiketh R. Potlapally, Naofumi Homma, Nicolas Sendrier, Nicolas Veyrat-Charvillon, Nigel P. Smart, Olivier Pereira, Orr Dunkelman, Palash Sarkar, Pankaj Rohatgi, Pascal Junod, Patrick Schaumont, Paulo S. L. M. Barreto, Phong Q. Nguyen, Pierre-Alain Fouque, Rainer Steinwandt, Ralf Kusters, Ran Canetti, Reihaneh Safavi-Naini, Renato Renner, Ricardo Dahab, Ron Steinfeld, Ronald Cramer, Rosario Gennaro, Scott Yilek, Serge Fehr, Sergei P. Skorobogatov, Sherman S. M. Chow, Shiho Moriai, Stefan Lucks, Stefan Mangard, Steven D. Galbraith, Subhamoy Maitra, Susan Hohenberger, Swarup Bhunia, Sylvain Guilley, T Gueneysu, Tal Malkin, Tatsuaki Okamoto, Tetsu Iwata, Thomas Eisenbarth, Thomas Johansson, Thomas Peyrin, Thomas Ristenpart, Thomas Roche, Thomas Shrimpton, Tomas Toft, Tsuyoshi Takagi, Vadim Lyubashevsky, Vincent Rijmen, Vinod Vaikuntanathan, Vipul Goyal, Wen-Guey Tzeng, Willi Meier, Xavier Boyen, Xiaoyun Wang, Yael Tauman Kalai, Yehuda Lindell, Yevgeniy Dodis, Yiorgos Makris, Yu Sasaki, Yuliang Zheng, Yuval Ishai, Zhimin Chen.