Updating the IACR Publication Infrastructure by a Preprint Server

Eli Biham
Computer Science Department
Technion – Israel Institute of Technology
Haifa 32000, Israel
biham@cs.technion.ac.il
http://www.cs.technion.ac.il/~biham/

Christian Cachin
IBM Research Division
Zurich Research Laboratory
CH-8803 Rüschlikon, Switzerland
cachin@acm.org
http://www.zurich.ibm.com/~cca/

August 9, 1999

Abstract

The publications sponsored by a scientific organization serve two main goals: fast publication of new research results and giving valuable credit to researchers for their works. The IACR is currently operating two levels for scientific publications: (1) the Journal of Cryptology publishes high-quality papers after a careful peer-reviewing process, and (2) the Crypto, Eurocrypt, and Asiacrypt (starting in 2000) conference series, in which authors present paper that are chosen by a program committee and proceedings are made available in Springer's LNCS series.

The current technology enables various other means for publication, which might serve the scientific community in addition to these established ways. Specifically, we propose to extend IACR's publishing activities through a preprint server for timely and rapid dissemination of new results. No refereeing will occur except for checking scope and superficial compliance with IACR's goals and the preprint server will be freely accessible over the Internet.

1 Introduction

Current technology affects the scientific publication process in various ways; with the current proliferation of the Web, for example, an author can publicize his work on his Web server, and allow other people to download copies of papers with only a few mouse operations. A more general service of this kind is a preprint server to which every author can send copies of his paper intended for wide dissemination, and everybody can see them and download and print copies. This serves the need of a very fast publication (even on the day of submission), but is essentially unrefereed.

IACR's main publishing activities are the Journal of Cryptology and the Crypto, Eurocrypt (and Asiacrypt starting in 2000) conference series with proceedings published by Springer in the Lecture Notes in Computer Science (LNCS) series. (In addition, IACR maintains the Newsletter and the Website `www.iacr.org` with focus on organizational rather than technical content.)

Journals are the oldest and most established form of scientific publication. They serve the need for archival publication of high-quality final results which pass a deep refereeing process, and meet journals editorial demands. The newer form of conference publications is generally faster; the contributions undergo a less careful peer-reviewing process. Conferences also enable frontal presentation of research results, but their publications serve the same goals as a journal with refereed publication of papers and giving credit to authors.

None of the two, however, guarantees particularly fast publication of the kind that authors expect today, and none of them allows giving credit to the authors of rejected papers. IACR conferences allow publication of a new result within several (6–12) months and the Journal of Cryptology has a backlog of one to two years.

It has become de-facto standard that IACR conferences accept and publish only a limited number of extended abstracts (typically between 30 and 40 papers of about 10–15 pages) and have rejection rates of 70%–80%. Each paper is given about 25–35 minutes for presentation; but the large share of rejected submissions are not published and face the risk of being lost (at least for IACR). Certainly, some of these submissions would not meet the necessary rigorous scientific standards and do not fit in high-quality conferences.

Some scientific associations, on the other hand, have conferences with, essentially, a free-speech policy and every paper whose correctness and quality is sufficient is published. Such a policy results in conferences with a huge number of presented papers, each is given only a few minutes, many of them are given in parallel in several conference rooms, and whose published proceedings allow only a limited number of pages per paper (in many cases only an abstract of one page). Typically, these fields have highly competitive journals.

In the recent years, the Internet has brought a third form of even faster publication to life: preprint servers. They serve the need for fast timely publications of research results, completely free of refereeing.

Such servers also allow publishing results in topics that are not well covered in the conferences due to small interest or other reasons of the program committees, and timestamp the results publicly in a way that is sometimes missing when submissions are made only to conferences.

In this note, we propose to update the IACR publication infrastructure by creating a new service of preprint server and we investigate its effect on existing publications and current policies, such as anonymous conference submissions.

2 A Preprint Server

The preprint server of IACR would operate as follows:

1. every author can submit a paper with a technical contribution in the field of cryptology;
2. the refereeing process is minimal: the only verification on the content of the paper is that it is really dealing with research in cryptology; no refereeing for quality or correctness is performed;
3. every submitter can remove his paper (for example if a mistake is found), but the server always keeps the title and abstract of the paper, and the reason for removal;
4. authors can update their papers at any time;
5. authors can add comments on the further history of the paper (such as a reference to publication in a journal or conference);
6. everybody can search the archive (by title, author, keyword ...), access all submissions, download and print copies;
7. everybody can subscribe to a daily (or weekly, monthly, depending on usage) mailing with new submissions.

These or similar functionalities already exist in other preprint servers. We now illustrate how such servers are already in use today, how IACR's server could be operated, how this server affects the research community in cryptology, the other publication efforts by IACR and the copyright issue, and the anonymous submission process.

3 Existing Preprint Servers

Preprint servers are already widely used in other fields; in Physics, for example, the Los Alamos e-print server `xxx.lanl.gov` has become the main source for accessing papers and announcing new results. The Los Alamos e-print server started in physics and was expanded to mathematics later and computer science recently. More than 100000 papers have been submitted since the service started in 1991 and there are more than 2000 submissions per month currently. The quantum physics part of the archive (`quant-ph`) contains 70–100 submissions per month in 1998.

The computer science part of `xxx.lanl.gov`, a.k.a. the Computing Research Repository (CoRR), has been established in late 1998 and is co-sponsored by ACM. It contains more than 30 subject areas in computer science; in particular also "Cryptography and Security". However, it has not been used much so far (there are less than 30 papers per month in all categories together).

There is already a small preprint server in cryptology, namely the "Theory of Cryptology Library" (`philby.ucsd.edu`), started by Oded Goldreich in 1996 and currently maintained by Mihir Bellare and Bennet Yee at UCSD. It lists 26 papers in 1998; many of them have appeared also (in shorter form) in IACR conference proceedings and some will appear in the Journal of Cryptology. Compared to the proposed IACR server, however, it seems that the Theory of Cryptology Library does not address the full scope of topics currently presented at IACR conferences. It can therefore only partially fulfill IACR's needs.

Of related interest, the Electronic Colloquium on Computational Complexity (`www.eccc.uni-trier.de/eccc/`) published 78 technical reports (preprints) in 1998.

4 Operation of the Server

A preprint server can be installed and maintained with not much overhead; the required expenses are expected to be much lower than those that IACR spends for conferences and for the Journal.

As for infrastructure, the service could be operated using the existing IACR account (currently hosted by `swcp.com`). Alternatively, commercial Web hosting services are available today starting at around $20/month and providing all needs to set up a sophisticated Web presence for about $100/month (e.g., `webhosting.com`). Hosting the service at a university is another option.

If the plan to install the preprint server is approved, we suggest that the IACR BoD appoints a responsible person as the maintainer of the preprint server (similar to the editor of the Journal of Cryptology and the editor of the IACR Newsletter). This would lead to a change of the IACR bylaws as well. The maintainer of the preprint server could appoint a small committee to share the work of checking submissions for conformance to the minimal requirements of the preprint server.

5 The Community

The lack of a preprint servers in cryptology has led various people to introduce partial solutions. One is the Theory of Cryptography Library mentioned above. Many people put their papers on their Web pages, and to access them, several directories of "cryptographers' homepages" have appeared and a huge meta-bibliography to papers available on personal pages has been compiled by Bruce Schneier (see `www.counterpane.com/biblio/`).

Personally, we know that hundreds of people are interested to receive announcements and copies on new papers (I keep a list of over 700 email addresses of people who *asked* that I will tell them when I have new papers – Eli).

There exist also several informal email distribution lists associated with particular research groups or institutions, to which announcements of talks, accompanying papers, or just new results are broadcast.

Crypto and Eurocrypt conferences have a traditional evening rump session, in which short announcements of recent research, quick ideas, and miscellaneous items are presented. In recent years, however, many people attempt to present their full research papers (that were not part of the conference program) in very limited time, just to get publicity. This has recently led to the typical 4-hr "monster session" with 7 minute presentations—not a very satisfying experience. We believe that this would change to the better if a general forum for timely research announcements is available.

All of these are further indications that IACR should start preprint server for cryptology.

A preprint server can also unite groups of researchers who would not have a common forum otherwise. For example, when four or five years ago the first breakthroughs in quantum computation occurred, there were only established publication tracks in Quantum Physics and in Theory of Computation. Because these did traditionally not have much interaction, the `quant-ph` section of the Los Alamos e-print server, which was new at that time, became the premier forum for that community.

6 Effect on Other Publications

Conference publication serves the need of frontal presentation of research results, along with refereed publication of good papers. IACR conferences are highly competitive as described above.

The Journal serves the need to archival publication of final results and full papers with a high quality and which pass refereeing review process and meets editorial standards. It is a pleasure to say that the Journal of Cryptology does a very good job of publishing high quality papers, where the careful refereeing process usually improves the accepted papers.

Because conferences are so competitive and the Journal is well-respected, we do not see any decrease in the number of submissions caused by a preprint server. In contrast, they will profit from each other.

Two issues have to be addressed, should the preprint server ever become the de-facto standard for publication in the field (i.e., every paper is submitted to the preprint server first): copyright and anonymous conference submissions. They are addressed next.

7 Copyright

A preprint server will clearly influence matters of copyright. For the Journal of Cryptology, the copyright is and has always been with IACR; for the Crypto and Eurocrypt proceedings published by Springer, authors have never assigned copyright to Springer up to now and a new model is currently being negotiated. IACR's clearly stated position is to ensure the widest spread of scientific ideas in the interest of its authors.

Articles in the preprint server will remain accessible on-line even after publication in a journal or proceedings volume. Some publishers might oppose this, as some even discourage authors from publishing their papers on their personal Web pages. Yet, one should not forget that the journal or conference publishing process still adds value to the work (it is a "final" version a and not a "preprint") and careful editing and typesetting takes place for publication in most journals.

This situation is, of course, not unique to IACR. We cite from a recent article in *Science* by members of the American Academy of Arts and Sciences' study on electronic communications "The Transition from Paper", who make a case for copyright assignment that guarantees wide distribution:

> Federal agencies that fund research should recommend (or even require) as a condition of funding that the copyrights of articles or other works describing research that has been supported by those agencies remain with the author. The author, in turn, can give prospective publishers a wide-ranging nonexclusive license to use the work in a value-added publication, either in traditional or electronic form. The author thus retains the right to distribute informally, such as through a Web server for direct interaction with peers. (...)
>
> Not-for-profit professional societies, as well as commercial for-profit publishers, will be divided in their reaction to this proposal. Some, such as Science, the New England Journal of Medicine, and the Journal of the American Chemical Society, have adamantly opposed authors' posting of their own articles on Web pages or e-print servers, whereas others, such as the American Journal of Mathematics, the Journal of Neuroscience, Nature Medicine, and Physical Review, have considered such distribution consistent with, and even advertising for, their own journals. [2]

We believe that IACR should continue to ensure the widest spread of scientific ideas. Currently, IACR pursues this goal through the contract with Springer (NY) for the Journal and through publishing the proceedings in the LNCS series by Springer (Germany). Springer is a commercial publisher and it is in IACR's interest that distribution by Springer works properly (because this serves IACR's own goals). If existence of the preprint server would make it impossible to continue these forms of publication, IACR would have to reconsider the *entire* question of it's publications. This could possibly lead to a more restrictive policy for the preprint server or to a radical change in publishing methods (e.g. Web instead of LNCS proceedings?).

However, drawing on the experience with preprint servers in other fields, we believe that the current Journal and LNCS paper publications will essentially remain unaffected by the preprint server.

8 Anonymous Conference Submissions

Since 1990, submissions to all IACR conferences have been anonymous (blind). This policy was adopted for various reasons, one being to ensure that program committee members do not prefer papers of their close colleagues over papers of less-known authors, another that the work of established researchers would not be treated favorably because of the author's fame alone, and to discourage any name-related discussion and selections.

Although this policy seems fair to outsiders, the program committee members identify authors successfully (even unintentionally) in many cases as they usually know the topics, current work, style, and language of their colleagues. Other unescapable hints to the authors are the references, the type of papers used in the authors' countries, etc.

Current fast publication speed allows authors to publicize their results widely in a matter of hours. The preprint server would provide such an opportunity. Some authors started to believe that anonymous submissions mean that they should delay any kind of publication of their paper, as they are not allowed to talk about their results, or to speak with committee members who work in their field; this, however, was never the intention of this policy.

On the contrary, the IACR's goals have always been that results should be published timely. This was confirmed by the IACR Board of Directors' meeting on May 2, 1999 in Prague:

> It was ensured that authors are allowed to announce their results in public when they are in an anonymous refereeing process, that they can tell (and give away papers to) colleagues who work on similar matters and should know about an author's results. If an author announces a result widely, and committee members are on the distribution list, they should not be removed just because the paper is in submission. Authors are allowed to give talks on their papers and submit them to existing preprint servers, which will usually be announced widely. On the other hand, it is not intended that a submitter send letters to all the committee members saying who wrote which paper. Anonymous submission just means that papers are submitted without author's names and too obvious references.

An IACR preprint server will not introduce fundamentally new problems for anonymous submissions; these problems exist already and if IACR does not have a preprint server, somebody else might. This illustrates just one of many ways in which the world has become smaller in the last then years.

Therefore, we believe that the anonymous submissions policy will become more and more difficult to maintain and should be reexamined. As we have argued, the question of an IACR preprint server should be considered separately from anonymity.

References

[1] Andrew M. Odlyzko, Papers on Electronic Publishing, http://www.research.att.com/~doc/eworld.html.

[2] "Who should own scientific papers?" S. Bachrach, R. S. Berry, M. Blume, T. von Foerster, A. Fowler, P. Ginsparg, S. Heller, N. Kestner, A. Odlyzko, A. Okerson, R. Wigington, and A. Moffat, Science 281 (no. 5382) (Sept. 4, 1998), pp. 1459-14. Accessible via [1].