Example of a Library Record
(revised)

Oded Goldreich
Department of Computer Science and Applied Mathematics
Weizmann Institute of Science
Rehovot, Israel.
E-mail: oded@wisdom.weizmann.ac.il

May 9, 1996

Abstract

This is merely an example for a file stored in the library. As an extra benefit it contains the first Call For Papers of the Library. The call describes the library's goals and its basic operations. Most importantly it describes the requested format of submissions. The only modification done in this revision is the addition of this sentence (but we certianly do not encourage such minor revisions in general...).

Introduction

In light of the enthusitic responses I've obtained from many of you, I hereby open the THEORY OF CRYPTOGRAPHY LIBRARY. At this stage the library operates with almost no software support and the services are minimal. The libarary site is http://theory.lcs.mit.edu/~cryptol and you are encourage to start submitting your relevant work by sending mail to cryptol@theory.lcs.mit.edu as descibed in the SUBMISSION INSTRUCTIONS enclosed below. In particular, you are encoureged to send two types of works

1. new work to be placed in the 1996 list of papers. (default)
2. old work, written before 1996 which have nevered appeared in a conference (with proceedings) or in a journal. Such work will be stored in the Archive (see below).

In addition, I've put all of you on the subscriber list. Subscribers will receive a monthly newsletter containing abstracts of all work recently placed in the library. I apologize to those not interested and ask them to notify me so that I can take them off the list.

P.S: My intention was to open these services ASAP and modify them as time goes along and the situation gets more clear.

Enclosed

1. A preliminary statment of Goals. Your comments are most welcome, especially w.r.t. the "definition" of Theory of Cryptography which was composed without too much thought.
2. A description of the basic operations of the library. Please note the SUBMISSION INSTRUCTIONS.

1 Goals and Policy

Our goal is to provide a forum for announcing new work in Theory of Cryptography and providing easy access to this work. Towards this end, we will store all relevant works which we receive and periodically notify the subscribers of new works received. For details on how to submit and subscribe to the library, see the *library's operation page* (enclosed below).

1.1 Scope

The library is intended to store works of interest to researchers interested in the theoretical aspects of Cryptography. We hope that we can handle the volume of work which falls into this category, but we certainly cannot handle at this stage larger volumes (e.g., all work in Cryptography). It is indeed hard to define what exactly constitutes a work in *Theory of Cryptography*, yet the following ingredients may give some idea.

- Establishing rigorous relations among natural cryptogarphic assumptions and objectives.
- Rigorously defined assumptions and models such as one-way functions, one-way permutations, trapdoor permutations, one-way hashing, claw-free permutation pairs, random oracle model, various types of adversaries (and restrictions on their behaviour),

- **Rigorous definitions of objectives** such as security of encryption schemes, chosen message attack, replay attacks, unforgeability of signatures and message-authentication, pseudorandom genrators and functions, zero-knowledge, commitment schemes, identification schemes, general multi-party computation, key-distribution problems, Oblivious Transfer, verifiable secret sharing, proactive security, non-interactive zero-knowledge, interactive proofs, proofs of knowledge, argument systems,

1.2 The Library's Policy

The library's policy is to accept every work within the above scope which may be of interest to the subscribers. Thus, our screening will be minimal (at the level of reading the abstract and checking that these conditions seems to be satisfied). We hope that we will never have to reject a submission.

We would prefer to receive full papers containing all essential details. However, we also welcome preliminary versions and extended abstracts. Revisions could be added at later stage.

1.3 The Library's Records

The library will consists of records, each record storing one work. The record will consist of a page containing the abstract, a link to the PostScript file of the full work, and the date the submission was received. In addition, there will be a page per each year listing all records of that year, and one **archive** page storing work prior to 1996 which were never published.

New work will be listed in the current year page. Unless indicated otherwise, we will assume that the submitted work is new.

The Archive: The archive is intended to store works written before 1996 which have never appeared in a conference (with proceedings) or in a journal. (Appearance as a Technical Report or as a *ECCC* report is fine, but do indicate this.) We ask authors of such works to indicate when the work was written. (We will not verify or vouch for this claim, but we feel it would be nice to include this claim in the work's record: see Operation.)

Revisions: In the future we will allow to submit revisions of work appearing in the library. It will be upto the authors whether to remove the original version (or other previous versions) or not. The library record will contain the dates of each version and pointers to the PostScript files (in case they were not removed). Further details will be worked-out in the future.

Removing a work: Authors can ask their work to be removed from the library at any time. Such a request will result in removing the PostScript file, but the record (with the abstract) will remain. Authors wishing to remove their work from the library are asked to indicate the reason for removal, which will be added to the record page. Potential reasons that we envision are a fatal flaw in the work and, conversely, its appearance in a conference with proceeding or a journal. We leave the decision of whether to remove a work which has been published in such form with the author. In particular, although we don't believe this may be the case, some publishers may insist on such removals in the future. Needless to say that we will appreciate if authors remove a work which is later found to be wrong.

1.4 The Library's Newsletter

Subscribers will receive a monthly newsletter listing the abstracts of work added to the library in the last two months.

2 Operation

In this preliminary stage, the library's operation is performed mainly by humans and so the services are quite minimal. We hope that in the future, somebody will volunteer to automate some of the proceess and upgrade the services provided.

You may submit work to the library and ask to remove it at any time. In case you remove your work, the library will only contain a record of your abstract. Your submission will not be refereed; we will only examine the abstract to verify that it seems to be within the intended scope and of potential interest to our subscribers.

2.1 How to submit work to be placed in the library

In order to submit a work you may simply send mail to `tcryptol@theory.lcs.mit.edu` with an abstract in clear (ASCII) text followed by a PostScript file. In case you wish to submit to the archive (see Goals above), please fill-in the comment field below. In case no other indication is given, we will assume the work to be new.
Please use a subject line indicating your desire that the work be placed in the library (e.g., "please place in library"). The subject line will be used in the receipt acknowledgement mail, so you may want to add some "key" specific to the submitted work.
Please use the following format in your submittion.

```
<b>title of your work</b>
<p>
<i>list of authors for the work</i>
<p>
<b>Abstract:</b>
Please keep your abstract short and informative.
It should be in clear (ASCII) test without any LaTeX commands.
Try to use no mathematical expressions.
If you have to use mathematical expressions please use a naive format
(of the kind used in the late troff as the LaTeX forms seem to upset
the various browsers).
For example, you may write $s sub 1 = sqrt(n)+t$.
<p>
<b>Keywords:</b>
Please use 2-5 keywords. We expect the following list to
suffice for most submissions within scope
(which can give you an idea of the scope we have in mind):
public-key, private-key, encryption, signatures, protocols,
message authentication, one-way functions, hard-core predicates,
pseudorandomness, zero-knowledge, commitment schemes, identification schemes,
key-distribution problems, chosen message attack, replay attack,
one-way hashing, universal hashing, collision-free hashing,
```

```
claw-free permutation pairs, trapdoor one-way permutations,
RSA, DES, factoring, Discrete Logarithm, Oblivious Transfer,
secret sharing, verifiable secret sharing, key escrow, proactive security,
interactive proofs, non-interactive zero-knowledge,
proofs of knowledge, argument systems, electronic cash,
general multi-party computation,
<p>
<b>comment:</b> in case of submission to the archive,
please indicate when the work was written.
(Please ignore minor revisions made at later dates.)
Also please supply citation to a prior Technical Report of this work
(resp. to a <A HREF=//www.informatik.uni-trier.de:/eccc/>ECCC</A> report)
in case either exists.
<p>
<b>contact author:</b> please supply one email address.
<p>
(The PostScript file of the full paper should follow here.)
<p>
```

2.2 Revisions

In the future we will allow to submit revisions of work appearing in the library.

2.3 How to remove your work from the library

In order to remove your work from the library simply send mail to `tcryptol@theory.lcs.mit.edu` indicating this wish and using the index assigned to your work. It will be nice if you also indicate the reason for removal. Potential reasons that we envision are a fatal flaw in the work and, conversely, its appearance in a conference with proceeding or a journal. We leave the decision of whether to remove a work which has been published in such form with the author. In particular, although we don't believe this may be the case, some publishers may insist on such removals in the future. Finally, let us stress that in case of removal, the library will still contain a record of the work consisting of the abstract and reason for removal.

2.4 Subscription to the library

Subscribers will receive a monthly list of abstracts of the new papers added to the library in the last two months. In order to subscribe or cancel your subscription to the library, simply send mail to `tcryptol@theory.lcs.mit.edu` indicating your wish.