How to Use the IACR Communications in Cryptology Class

iacrcc LaTeX Class Documentation (v0.61)

Joppe W. Bos[1] and Kevin S. McCurley[2]

[1] NXP Semiconductors, Leuven, Belgium
[2] Self, United States

Abstract. This document is a quick introduction to the `iacrcc.cls` LaTeX class for the IACR Communications in Cryptology.

Keywords: Template · LaTeX · IACR

Introduction

This document is a guide to preparing a paper for the IACR journal titled "IACR Communications in Cryptology". Papers for the journal must be prepared in LaTeX using the `iacrcc` document class. The biggest difference between `iacrcc` and other classes you may have used is the way in which metadata is supplied (e.g., title, author information, affiliations, and funding information). Our goal is to minimize the amount of human effort required to process final versions of a paper, so that we can reduce the cost of open access publishing. Some of the stylistic choices were inspired by IACR Transactions class file (the `iacrtrans` class v. 0.92) written by Gaëtan Leurent and Friedrich Wiemer with help from others.

The class is still in development and feedback and comments are welcome. The latest version can be found at: `publish.iacr.org/iacrcc`. There is also a github repository where you can open issues or to submit pull requests. The complete package consists of three files. `iacrcc.cls` is the main document class. `iacrdoc.tex` is used to produce this PDF file. `template.tex` can be used as a starting point for writing a paper. The LaTeX source of `iacrdoc.tex` can also be used as a more advanced example, but please make sure to remove any unnecessary code.

NOTES

- The production system to which you submit your final version requires that the main LaTeX file should be `main.tex`. You might as well start that way by copying `template.tex` to `main.tex`.
- The default fonts are provided by the `lmodern` package. Do not change this.
- Avoid using too many packages. Many authors are lazy and just copy what they used in the past. Some won't work - see the list of acceptable packages at `https://publish.iacr.org`. Don't use any package that changes fonts.

This is a generic footnote produced with `\genericfootnote{...}`.

E-mail: `joppe.bos@nxp.com` (Joppe W. Bos), `iacrdoc@digicrime.com` (Kevin S. McCurley)

Date of this document: 2024-03-25.

- Don't try to change the `hyperref` options, the bibliography style, the page style, or the page numbering.
- Don't use macros like `\if` or `\include` inside any metadata like the title or abstract.
- Footnotes are handled differently in this class, and in particular `\thanks` is disabled.

1 Invocation and usage

The class supports the following class options with `\documentclass{iacrcc}`

`[version=preprint]` for preprints (without copyright info, default)

`[version=submission]` for submissions (anonymous, with line numbers). If desired, this can be combined with `[notanonymous]` if the call for papers requires non-anonymous submissions.

`[version=final]` for final papers. This imposes some additional requirements.

`[biblatex]` may be used if you prefer using BibLaTeX to BibTeX. Note that we do not support options to be passed to BibLaTeX, as they may conflict with the style of the journal. We use a bibliography style based on the alpha style (e.g., [RSA78]).

`[floatrow]` load the `floatrow` package. This is useful when you have fancy figures or tables. In either case, `iacrcc` will customize how tables and figures are laid out.

An example how to pass an option to this document class is `\documentclass[version=submission]{iacrcc}` for submissions.

Before submitting your final version, please make sure that it compiles properly with the `[version=final]` option and check that the author names and affiliations are correct and a text version of the abstract is provided in the `textabstract` environment.

The current date of compilation time is automatically added to the footer of the front page. If you want to adjust this date you can use the `\documentdate` macro (e.g. `\documentdate{2023-10-05}`) or use `\documentdate{}` to omit adding the date.

The `iacrcc` class automatically loads `hyperref` after all other packages. If you need some packages to be loaded *after* `hyperref`, you should read Section 5.

2 Macros to add title and author information

2.1 Title

A title is added using the `\title` macro, it has a number of optional arguments:

`running`	The running title displayed in the headers.
`plaintext`	A text version of the title (mandatory if macros are used in the title).
`subtitle`	Provide a subtitle.

An example using all the optional arguments would look like:

```
\title[running   = {How to use the iacrcc class},
       plaintext = {How to use the iacrcc LaTeX class},
       subtitle  = {A Template},
      ]{How to use the \texttt{iacrcc} \LaTeX\ class}
```

The `plaintext` option is only required if you use macros in your title (it is required in the example). Inline mathematics and accents like `\"u` are allowed in plain text. Note that LaTeX has defaulted to UTF-8 input since 2019, so just ü is preferred to `\"u`. Note that `\thanks` and `\footnote` are disabled and you should instead use the `\genericfootnote` macro described in section 2.5.

2.2 Authors

Author information is entered using the `\addauthor`, `\addaffiliation`, and `\addfunding` macros. Authors are asked to enter this information in a structured way so that we can provide it to indexing agencies. The `\author` macro is disabled.

Authors are listed individually using repeated calls to the `\addauthor` command. There are a number of optional arguments to `\addauthor`:

`inst`	A numerical list of indices specifying an institution in the affiliation array (see below).
`orcid`	Create a small clickable orcid logo next to the authors name looking like and linking to the authors ORCID (see: https://orcid.org).
`footnote`	Create an author-specific footnote.
`surname`	Indicate the surname of the author for indexing purposes.
`onclick`	Provide a URL to visit when clicking on the external link logo displayed next to the author name: e.g., can point to the academic webpage.
`email`	Define the e-mail address of this author. Note that at least one e-mail address is required when `[version=final]` is used.

We **strongly** recommend that authors enter their ORCID ID into the paper, because this ensures that they will get citation credit for their papers. Authors can use the `\surname` macro to indicate what part of the author name is the surname: this is used for meta-data collection and is especially useful for cases with middle names *and* double surnames which might be confusing.

When the URL provided to the `onclick` option contain characters with a "special" meaning in LaTeX they might render incorrectly. An example with some of the common characters ~, %, and # is

```
onclick = {https://www.webpage.com/\string~\%\#/}
```

which displays next to the author name.

An example using all the optional arguments is given below. In this case the author has `inst={1,2}` to indicate that they are affiliated with the first and second affiliations that are entered with `\addaffiliation`:

```
\addauthor[orcid    = {0000-0000-0000-0000},
           inst     = {1,2},
           footnote = {Thanks to my supervisor for the support.},
           onclick  = {https://www.mypersonalwebpage.com},
           email    = {alice@accomplished.com},
           surname  = {Accomplished},
          ]{Alice Accomplished}
```

The author names displayed in the header are constructed automatically for four authors or less. One can optionally modify this with the `\authorrunning` macro. For five or more authors the use of the `\authorrunning` macro is mandatory. The `\thanks` macro is disabled inside `\addauthor`, so use the `footnote` option on `\addauthor` instead.

2.3 Affiliations

Affiliations are listed individually using the `\addaffiliation` command *after* the last author has been added using `\addauthor`. There are a number of optional arguments to `\addaffiliation`:

`ror`	Provide the Research Organization Registry (ROR) indentifier for this affiliation (see: https://ror.org). This is used for meta-data collection only.
`department`	Department or suborganization name.
`street`	Street address.
`city`	City name.
`state`	State or province name.
`postcode`	Zip or postal code.
`country`	Country name. Required for `[version=final]`.

There is an online tool at publish.iacr.org/funding to help you find ROR identifiers, and you are strongly urged to include these. Country is required if `[version=final]` on the paper. When provided, only the `city` and `country` arguments are used to display the affliation. The other arguments are used to provide to indexing agencies. An example using all the optional arguments would look like:

```
\addaffiliation[ror        = {05f950310},
                department = {Computer Security and Industrial Cryptography},
                street     = {Kasteelpark Arenberg 10, box 2452},
                city       = {Leuven},
                state      = {Vlaams-Brabant},
                postcode   = {3001},
                country    = {Belgium}
               ]{KU Leuven}
```

2.4 Funding information

Authors should use the `\addfunding` macro to make sure that funding agencies can find papers published under their sponsorship. An example is:

```
\addfunding[fundref = {100000001},
            grantid = {CNS-1237235},
            country = {United States}]{National Science Foundation}
\addfunding[ror     = {00pn5a327},
            country = {United States}]{Rambus}
```

In this example, the author acknowledges a grant from the National Science Foundation and support from Rambus (with no `grantid`). The inclusion of funding from an agency without a `grantid` might be appropriate if the author simply received support for a visit.

The complete list of optional arguments for `\addfunding` is:

`fundref`	An identifier from the Crossref funder registry.
`ror`	An identifier from the Research Organization Registry (ROR). A `fundref` identifier is preferred for `\addfunding`.
`country`	The country of the funding agency.
`grantid`	The identifier of the grant that is assigned by the agency who provided it.

You can use the online tool at publish.iacr.org/funding to help you find `fundref` and `ror` identifiers.

Note that `\addfunding` **does not** automatically create footnotes or an acknowledgements section to identify funding - it only collects the metadata for indexing. If you wish to include such visible annotations, you can use the `footnote` option on `\addauthor`, or the `\genericfootnote`, or add a separate acknowledgements section. Some funding agencies have specific requirements for how they want to be acknowledged in the paper.

2.5 Footnotes

Authors may be accustomed to using `\thanks` for footnotes indicating affiliation, email, or funding, but the `\thanks` macro is disabled and you should use other methods described in this document.

- Footnotes on titles are not supported. You should use `\genericfootnote` to place a footnote on the first page without a reference. This is useful to indicate this is a full / extended version of a published paper, or to indicate funding relationships for the authors. This is an optional macro that may be repeated for multiple footnotes.
- For a footnote on an author, use the `footnote` option on `\addauthor`. This can be used for indicating that the author's affiliation for the work was different than their current affiliation, or to indicate contact address, or a previous name, etc.

Footnotes may be used elsewhere in the paper, but please do not overuse them.

2.6 License

When the `version=final` document mode is used, the author needs to provide a supported license. In all other modes this information is not required and is ignored if it is provided. At present the only acceptable license is `CC-by`. An example would look like:

```
\license{CC-by}
```

2.7 Keywords

Use `\keywords{keyword1, keyword2}` to give a list of keywords or key phrases. This is an optional macro that should appear before the abstract. Individual keywords should be separated by commas. If the argument to `\keywords` contains math or macros, then you must supply an additional set of text-only keywords; for example:

```
\keywords[rings, arithmetic on Z]{rings, arithmetic on $\mathbb{Z}$}
```

2.8 Abstract

Abstracts serve several purposes in a journal article, including both summarization and indexing. An abstract should be a self-contained mini-document that describes the contributions of the paper. It should be free of bibliographic references and also free of undefined terminology introduced in the paper. It is acceptable to use mathematical notation, but this kind of content is not useful for indexing.

For this reason, the `iacrcc` document class uses two kinds of abstracts. The first (traditional) form of abstract is entered with the `abstract` environment as usual. Note that the keywords should be given before starting the `abstract` environment.

For `final` versions of papers, an additional "text-only" abstract is required. This abstract is contained in the `textabstract` environment, and should not contain user-defined macros. It will be used for indexing and production of HTML pages to describe the paper. As such, it is just as important as the classical `abstract` of a paper because it contains a textual summary that readers will use to decide if the paper is worth reading.

The only difference is that the contents of the `textabstract` is constrained on what it may contain.

You may use unicode such as in `Paul Erdős` or diacriticals like `F\"ur Elise`. You may also use inline or display mathematics in the `textabstract` environment as well as (for example) the `itemize` environment. User-defined macros are *not* allowed. We do not have a complete list of allowed LaTeX(which can be succesfully converted to HTML) but but you will find out when you upload your final version at https://publish.iacr.org.

The contents of this environment will be written to a file that ends with `.abstract` when you compile your LaTeX, but will not be displayed in the final PDF except as metadata. Note that `\begin{textabstract}` must appear on a line by itself.

2.9 Theorems

The `iacrcc` class uses the $\mathcal{AMS}$ packages to typeset math. In particular, it loads the `amsthm` package, and predefines the following environments:

`theorem`	`definition`	`remark`
`proposition`	`example`	`note`
`problem`	`exercise`	`case`
`lemma`	`property`	
`conjecture`	`question`	
`corollary`	`solution`	
`claim`		

Note that the `proof` environment automatically adds a QED symbol at the end of the proof. If the QED symbol is typeset at a wrong position, you can force its position with `\qedhere`.

3 Auxiliary files

One goal of the `iacrcc.cls` file is to automate the production of machine-readable metadata in separate files. Users of LaTeX will already be used to seeing this with the `.log`, `.aux`, `.bbl`, `.blg`, `.toc`, and `.out` files produced by BibTeX and the `hyperref` package. You need not be concerned about these, but if your main LaTeX file is called `main.tex`, then the extra files that are produced are:

- a flat text file `main.meta` containing all metadata from the paper. When you compile `main.tex`, it will produce the metadata from `main.tex`, and when you run `bibtex` and `latex` again, it will append the citation data from BibTeXinto the `main.meta` file as well.
- a file `main.abstract` that contains the contents of the abstract for the paper provided with the `textabstract` environment. This will be used to show the abstract on the web.

4 Typesetting the Bibliography

Having good bibliographic references is very important for the visibility of the journal. Since we don't use a commercial editor, authors need to make sure themselves that references are standardized and clean. We strongly encourage authors to use bibliographic data from http://www.dblp.org or https://cryptobib.di.ens.fr/. All references should have DOIs if at all possible.

You must use either BibTeX or BibLaTeX; you may not format your own bibliography. If you use BibTeX, then the `iacrcc` class will load the `\bibliographystyle{alphaurl}`

style. You may not change this. If you use BibLaTeX, then this is done using `\documentclass[biblatex]{iacrcc}` instead of `\usepackage{biblatex}`; the latter will generate an error because the `iacrcc.cls` file loads BibLaTeX with a specific style.

Here are some example citations: the RSA paper [RSA78], the AES standard [NIS01], and [Koc96].

For the IACR Communications in Cryptology, you will be required to upload your BibTeXfiles rather than just the `bbl` file. Many authors use the `cryptobib` BibTeX files, and you need not upload those with your paper. They can be referenced as `\bibliography{cryptobib/abbrev1,cryptobib/crypto}`

5 Package load order

LaTeX suffers from the weakness of having a global namespace for macros. As a result, it is possible that some packages may overwrite the definitions of another package that was loaded earlier. The biggest offender for this seems to be the `hyperref` package, which overwrites some basic macros in LaTeX itself. The `iacrcc` document class loads `hyperref`, but it provides a mechanism for loading packages *after* `hyperref`. If the file `after-hyperref.sty` exists in the directory of your main file, then it will be included after loading `hyperref`. As an example, to load `cleveref` after `hyperref`, you can create a file `after-hyperref.sty` that contains:

```
\RequirePackage{cleveref}
```

A complete survey of the conflicts between packages is beyond the scope of this document, but some known conflicts between packages are documented in the `pkgloader` package. It is wise to read the documentation for any package you use to make sure there are no conflicts with other packages loaded by `iacrcc.cls`.

6 Some recommendations

LaTeX distribution, and worklow. LaTeX distributions are available on a variety of platforms. In particular, we recommend the TeX Live distribution, which is updated regularly, includes a large number of packages, and is available on many platforms. We use the texlive medium scheme in our cloud service to compile final versions of papers.

Pictures. We recommend the use of the `tikz` package to render pictures. In particular, a large variety of crypto pictures made with `tikz` is available at `iacr.org/authors/tikz/`

External pictures. The `graphicx` is loaded by the class, and is recommended for external figures. The submission server does not support `svg` format for included graphics, so you should convert `svg` files to a supported format. If possible, external figures should be in a vector format (PDF or EPS). Note that the `\includegraphics` command will automatically select a file with what it thinks should be the right extension, so if you write `\includegraphics{figure}` and have two files `figure.gif` and `figure.eps`, it will try to select the correct one.

Floats. Figure captions should be below the figures, and table captions above the tables. The `float` package loaded by the class should take care of this automatically. If want to have several figures side by side, see the `[floatrow]` option.

Tables. We recommend the `booktabs` package to typeset tables.

Algorithms. We recommend the `algorithmicx` packages for algorithms (in particular, `algpseudocodex` for pseudo-code).

7 Further information

If you are a LaTeX novice, you may wish to consult the following documents:

- General LaTeX documentation, such as the (not so) short introduction to LaTeX 2_ε;
- The amsmath documentation is useful for learning how to typeset mathematics.

Sample References

[Koc96] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer, 1996. doi:10.1007/3-540-68697-5_9.

[NIS01] National Institute of Standards and Technology. *Announcing the Advanced Encryption Standard (AES)*, 2001. Federal Information Processing Standards Publication 197, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. doi:10.1145/359340.359342.