IACR Transactions

LETEX Class Documentation (v. 0.93)

Gaëtan Leurent¹ and Friedrich Wiemer²

Inria, Paris, France, gaetan.leurent@inria.fr
 Ruhr-Universität Bochum, Bochum, Germany, friedrich.wiemer@rub.de

 $\mbox{\bf Abstract.}$ This document is a quick introduction to the LATEX class for the IACR Transactions.

Keywords: IACR Transactions \cdot ToSC \cdot TCHES \cdot LATEX

Contents

Introduction

The iacrtans LaTeX class is used by the new "IACR Transactions" journals ToSC (IACR Transactions on Symmetric Cryptology) and TCHES (IACR Transactions on Cryptographic Hardware and Embedded Systems). The class is based on standard LaTeX classes and packages (mainly the article class with amsmath), and should be similar in use to the llncs class used for Springer's proceedings.

The class is still in development and feedback and comments are welcome. The latest version can be found on the Github page of the project: https://github.com/Cryptosaurus/iacrtrans, feel free to open tickets for issues or to submit pull requests.

1 FAQ: Frequently Asked Questions

1.1 Converting llncs papers to iacrtrans for submission

If you have a paper typeset with the llncs class, conversion should be relatively easy. The following steps should be sufficient in most cases (for the submission version):

- Replace \documentclass{llncs} with \documentclass[journal=XXX,submission,spthm]{iacrtrans}, where XXX is either tosc, or tches;
- 2. Replace \bibliographystyle{splncs03} with \bibliographystyle{alpha};
- 3. Add a \keywords{} command before the abstract, with keywords separated by \and;
- 4. Remove commands that might override the class style, such as \pagestyle{...} or \thispagestyle{...}, change of margins (e.g. with the geometry package), change of fonts, ...
- 5. See also ?? for information about how to typeset the bibliography.

1.2 Template file

There is a template.tex file included with this class, to use as a starting point for writing a paper. The LATEX source of this documentation can also be used as a more advanced example, but please make sure to remove any unnecessary code.

1.3 Preparing the final version

Before submitting your final version, please make sure that it compiles properly with the [final] option (see the next subsection in case of issues), and check that the author names and affiliation are correct. In particular, each affiliation MUST be of the form (institue), (city), (country).

1.4 Compilation issues

If your document doesn't compile with the iacrtrans class, you can try adding the [nohyperref] option. This will disable some code in the class that is known to be fragile, in particular the generation of metadata. If this fixes your compilation problems, please try to define a clean version of author, institute, title and/or keywords as optional arguments to these commands (in particular, remove LATEX macros, and write everything on a single line), and see if you document now compiles without the [nohyperref] option.

1.5 Line number issues

In submission mode, the class adds line numbers to help reviewers refer to specific elements. Unfortunately, the code that does this is rather fragile, and some constructions break the line numbering. In particular, old-style equations with \$...\$ are known to cause issues, please use $\{\ldots, \}$ instead¹.

If you find other cases where line numbering is broken, please open a ticket on github, and we will try to find a solution when possible. As a quick workaround, you can wrap the offending environment with \begin{linenomath} / \end{linenomath} (this will do nothing in preprint or final mode when line numbers are deactivated).

2 Main Commands

2.1 Title page

The following commands are used to input informations for the title page.

\title to define the title.

A shorter running title can be given as optional argument.

\subtitle to give an optional subtitle.

\author to define the author list.

Author names must be delimited by \and macros. If there is one different affiliation for each author, authors and affiliations will be numbered automatically. Otherwise, each author name must be followed by \inst{...} with the corresponding affiliation(s).

A shorter list of authors for the running head can be given as optional argument.

¹For more background on \$\$...\$\$ and \[...\], see https://tex.stackexchange.com/questions/503/why-is-preferable-to

\institute to give author's affiliation(s).

If there are several affiliations, they must be separated by \and macros, and will be numbered automatically.

\keywords to give a list of keywords.

Individual keywords should be separated by the \and macro.

If there are fragile commands in the keywords, use the optional argument to give a text-only version of the keywords; this will be used for the PDF metadata.

\email should be used inside the **\institute** argument to typeset author's email address(es). An optional argument can be given for the hyperlink, if different from the displayed email. For instance, you can group emails as follows:

\email[alice@foo.com,bob@bob.com]{{alice,bob}@foo.com}

\thanks can be used inside the **\title**, **\author** or **\institute** argument to generate a footnote with additional information, if needed.

\maketitle is used to actually typeset the title.

The abstract environment should be used to typeset the abstract.

Note that the keywords should be given before starting the abstract environment.

2.2 Theorems

The iacrtrans class uses the $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ 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 (unless you give option [spthm] to the iacrtrans class). If the QED symbol is typeset at a wrong position, you can force its position with \qedhere.

3 Class options

3.1 Publication type

The class supports four publication types, selected with the following class options:

[final] for final papers

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

[submission] for submissions (anonymous, with line numbers)

[draft] is similar to preprint, but activates draft mode for the underlying article class (which shows overfull hboxes), and other packages (e. g. graphicx, hyperref).

Some types supports further options:

[journal=XXX] must be used for submissions and final papers; allowed values are tosc and tches, to set the publname macro accordingly to the right journal

[notanonymous] can be used in submission mode, when the call for paper requires non-anonymous submissions.

3.2 Other Options

\end{document}

[spthm] provides theorem environments that emulates llncs class's sptheorem:

- A \spnewtheorem wrapper is provided around AMS \newtheorem. Note that the styling options are ignored; you should use standard amsthm commands for fine control.
- The $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ proof environment will not automatically add a QED symbol at the end of the proof.

[floatrow] uses the floatrow package to customize floats rather than the plain float package. In particular, this allows to typeset floats side by side as shown in this example:

```
\documentclass[floatrow]{iacrtrans}
\usepackage[demo]{graphicx}
\begin{document}

\begin{figure}
  \begin{floatrow}
  \ffigbox{\includegraphics[width=0.4\textwidth]{1.png}}
  {\caption{This is caption 1.}}
  \ffigbox{\includegraphics[width=0.4\textwidth]{2.png}}
  {\caption{This is caption 2.}}
  \end{floatrow}
\end{figure}
```

The row will be divided equally according to the number of figures, but you can ask each figure to take its natural space instead with \ffigbox[\FBwidth]. For more advanced use, see the floatrow documentation.

[xcolor=\(\lambda \) ist of options\(\rangle] passes \(\lambda \) ist of options\(\rangle\) to the xcolor package. Since xcolor is loaded by the class, you have to use this mechanism to pass options at load time; for instance use xcolor=svgnames to load SVG color names.

[hyperref=(list of options)] passes (list of options) to the hyperref package. Alternatively, you can load hyperref yourself with the required options and the class will detect that it already loaded.

[nohyperref] disables the automatic loading of hyperref. Use this is if your document fails to compile with hyperref for some reason.

The iacrtrans class automatically loads hyperref after all other packages. If you need some packages to be loaded *after* hyperref, you should load hyperref explicitly at the correct position, but not use the [nohyperref] option.

[nohyperxmp] disables the automatic loading of hyperxmp. The iacrtrans class has issues with hyperxmp versions between 5.0 and 5.4, use this option to disable loading it.

[nolastpage] disables the automatic loading the lastpage package in [final] mode. When this option is enabled, the last page number must be set explicitly with \setlastpage.

4 Typesetting the Bibliography

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

We are still working on a good solution for the bibliography, and we expect to have more specific instructions when producing the final version of the papers, including a dedicated $BibT_{EX}$ style.

5 Further instructions

ETEX distribution, and worklow. IATEX distributions are available on a variaty of platforms. In particular, we recommand the TeX Live distribution, which is updated regularly, include a large number of packages, and is available on many platforms.

Linux: A LaTeX installation is included in most Linux distributions. Alternatively, TeX Live can be installed easily without root access.

Windows: There are also good LATEX distributions for Windows, such as MikTeX and TeX Live.

MacOSX: On MacOSX, TeX Live is available inside MacTeX.

We recommand the use of pdflatex because it generally supports more features than latex and dvips (xelatex and lualatex are also missing some advanced features from pdflatex).

Internal references. We recommend the use of \autoref from hyperref (automatically loaded by the class). For instance, \autoref{sec:options} links to ??.

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 http://www.iacr.org/authors/tikz/.

External pictures. The graphicx is loaded by the class, and is recommended for external figures.

If possible, external figures should be in a vector format: you can use PDF files when compiling with pdflatex, and EPS files when compiling with latex, and dvips. Note that the \includegraphics command will automatically select a file with the right extension, so if you write \includegraphics{figure} and have two files figure.pdf and figure.eps, it should work with both workflow.

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 algorithm, algorithmex packages for algorithms (in particular, algorithms, algorithmed).

6 For the Editor

The following commands should be used by the editor to prepare the final version:

- \setfirstpage to set the first page number.
- \setlastpage to set the last page number (optional).
- \setvolume to set the volume number.
- \setnumber to set the edition number.
- \setDOI to set the DOI.
- \setPublished to set the publication date.
- \setAccepted to set the notification date.
- \setRevised to set the re-submission date for paper that went though major revision.
- \setReceived to set the submission date.

There is a special settings.tosc.tex file, that sets default values for these commands and which can be included in the beginning of the main tex file.

7 Further information

More general information can be found in the following documents:

- General LATEX documentation, such as the (not so) short introduction to LATEX 2;
- The AMS-IATEX documentation and amsthm documentation;
- Documentation of the LATEX packages used in the class (see below).

7.1 Packages used

The class is based on the standard article class, and loads the following packages:

- geometry, sectsty, fancyhdr, float, microtype, fontenc, lmodern
- amsmath, amssymb, amsthm, mathtools
- graphicx
- xkeyval, afterpage
- hyperref, hyperxmp, etoolbox, xcolor (unless the [nohyperref] option is used)
- lineno (in [submission] mode)
- lastpage (in [final] mode, unless disabled with [nolastpage])
- floatrow, caption (with option [floatrow])

Thanks

We would like to thank people who helped design and improve the class: Anne Canteaut, Jérémy Jean, Marc Joye, Bart Preneel, Christian Rechberger, Tyge Tiessen, Jonas Wloka.

Changes

- v 0.21 First public version
- ${f v}$ 0.22 Added documentations. Minor tweaks in the class.
- v 0.23 More documentation. Removed some extra line-numbers with AMS environments in submission mode. Make autoref capitalize sections. Table caption are now above tables. Rewritten running authors and running title. Added PDF info (title, author, keyword). Optional argument for \email. Added floatrow option.
- ${\tt v}$ **0.24** Added CC licence text, and added XMP metadata. Fixed some metadata transformations.
- v 0.26 Added ISSN number and fixed a few bugs with spthm (thanks to Marc Joye).
- v 0.27 Added paragraph Helping the editor in the documentation, added settings.tosc.tex.
- v 0.90 Moved to github, various fixes. Added journal class option to switch between TCHES and ToSC. Changed default mode to preprint.
- v 0.91 Adding publication in the final version. Added new class options: notanonymous, xcolor=xxx, hyperref=xxx, nolastpage.
- \mathbf{v} **0.92** Fixed hyperxmp issues. Added template for authors.
- **v 0.93** Fixed bug with affiliation footnote numbering for more than 10 affiliations. Fixed hyperxmp issues (new issues with version 5.12). Added new class option nohyperxmp.