

# IACR Transactions on Symmetric Cryptology

## L<sup>A</sup>T<sub>E</sub>X Class Documentation (v. 0.24)

Gaëtan Leurent<sup>1</sup>, Alice<sup>2</sup> and Bob<sup>2</sup>

<sup>1</sup> Inria, France, [gaetan.leurent@inria.fr](mailto:gaetan.leurent@inria.fr)  
<sup>2</sup> ACME

**Abstract.** This document is a quick introduction to the L<sup>A</sup>T<sub>E</sub>X class for the IACR Transactions on Symmetric Cryptology.

**Keywords:** IACR Transactions on Symmetric Cryptology · ToSC · L<sup>A</sup>T<sub>E</sub>X

## Introduction

The `iacrtans` L<sup>A</sup>T<sub>E</sub>X class will be used by the new “IACR Transactions on Symmetric Cryptology” journal. The class is based on standard L<sup>A</sup>T<sub>E</sub>X 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 L<sup>A</sup>T<sub>E</sub>X source of this documentation is meant as an example to show basic usage of the class.

Since we are now preparing the zero-th issue of the journal, the class is still in development and feedback and comments are welcome.

## FAQ: Converting `llncs` papers to `iacrtrans`

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):

1. Replace `\documentclass{llncs}` with `\documentclass[submission,spthm]{iacrtrans}`;
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 Main Commands

### 1.1 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.

`\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 meta-data.

`\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.

## 1.2 Theorems

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

<code>theorem</code>	<code>definition</code>	<code>remark</code>
<code>proposition</code>	<code>example</code>	<code>note</code>
<code>problem</code>	<code>exercise</code>	<code>case</code>
<code>lemma</code>	<code>property</code>	
<code>conjecture</code>	<code>question</code>	
<code>corollary</code>	<code>solution</code>	
<code>claim</code>		

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`.

## 2 Class options

### 2.1 Publication type

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

**[final]** for final papers (default mode)

**[preprint]** for preprints (without copyright info)

**[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`).

## 2.2 Other Options

**[spthm]** provides theorem environments that emulates `llncs` class's `spttheorem`:

- A `\spnewtheorem` wrapper is provided around  $\mathcal{AMS}$  `\newtheorem`. Note that the styling options are ignored; you should use standard `amsthm` commands for fine control.
- The  $\mathcal{AMS}$  `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}

\end{document}
```

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.

**[nohyperref]** disables the automatic loading of `hyperref`. Use this 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.

## 3 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 bibliography, 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 `BIBTeX` style.

## 4 Further instructions

**L<sup>A</sup>T<sub>E</sub>X distribution, and workflow.** L<sup>A</sup>T<sub>E</sub>X distributions are available on a variety of platforms. In particular, we recommend 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 L<sup>A</sup>T<sub>E</sub>X distributions for Windows, such as [MikTeX](#) and [TeX Live](#).

**MacOSX:** On MacOSX, TeX Live is available inside [MacTeX](#).

We recommend 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`, `algorithmcx` packages for algorithms (in particular, `algpseudocode` for pseudo-code).

## 5 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 first page number (optional).

`\setvolume` to set the volume number.

`\setnumber` to set the edition number.

`\setDOI` to set the DOI.

## 6 Further information

More general information can be found in the following documents:

- General L<sup>A</sup>T<sub>E</sub>X documentation, such as the (not so) short introduction to L<sup>A</sup>T<sub>E</sub>X 2<sub>ε</sub>;
- The  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X documentation and amsthm documentation;
- Documentation of the L<sup>A</sup>T<sub>E</sub>X packages used in the class (see below).

### 6.1 Packages used

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

- `geometry`, `secsty`, `fancyhdr`, `mathtools`, `float`, `microtype`, `lastpage`
- `amsmath`, `amssymb`, `amsthm`
- `graphicx`
- `hyperref`, `hyperxmp`, `etoolbox`, `xcolor` (unless the `[nohyperref]` option is used)
- `lineno` (in `[submission]` mode)
- `floatrow`, `caption` (with option `[floatrow]`)

## Thanks

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

## Changes

**v 0.21** First public version

**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.

**v 0.24** Added CC licence text, and added XMP metadata. Fixed some metadata transformations.