TamKang University
Department of Electrical Engineering
Laboratory of Cryptography and Information Security

LCIS

Technical Report

TR-doc-0.4

LaTeX 2$_\varepsilon$ Class for LCIS Technical Reports (version 0.4)

Marc Joye

March 31, 1998

LaTeX 2ε Class for LCIS Technical Reports (version 0.4)

Marc Joye

March 31, 1998

Dept of Electrical Engineering, Tamkang University
Tamsui, Taipei Hsien, Taiwan 25137, R.O.C.
Email: joye@ee.tku.edu.tw

Abstract. This document explains how to prduce a technical report for the LCIS. If you are already familiar with LaTeX, then the `lcistech` class should not give you any major difficulties. Some extra commands and macros, which are not provided by LaTeX (e.g. `\institute`, `\LCIS`) are available.

1 How to Proceed

The `lcistech` class is an extension of the standard LaTeX `article` document class. Therefore you may use all "article" commands for the body of your contribution to prepare your report. The `lcistech` class is invoked by replacing "article" by "lcistech" in the first line of your document:

```
\documentclass{lcistech}
%
\begin{document}
  <body of the report>
\end{document}
```

If a report without title page is desired, then the option `notitlepage` should be passed to the class:

```
\documentclass[notitlepage]{lcistech}
```

Please refrain from using any LaTeX or TeX commands that affect the layout or formatting of your document (i.e. commands like `\textheight`, `\pagestyle` etc.).

TR-doc-0.4

2 How to Code the Beginning of Your Report

The title of your report (it is mandatory) should be coded as follows:

```
\title{<your title>}
```

All words in titles should be capitalized except for conjunctions, prepositions (e.g. on, of, by, and, or, but, from, with, without, under) and definite and indefinite articles (the, a, an) unless they appear at the beginning. Formula letters must be typeset as in the text. Titles have no end punctuation.

For long titles that do not fit in the single line of the running head, you can specify an abbreviated title for the running head with the command:

```
\title[<your abbreviated title>]{<your title>}
```

Now the name(s) of the author(s) must be given:

```
\author{<author(s) name(s)>}
```

Numbers referring to different addresses or affiliations are to be attached to each author with the `\inst{<no>}` command. If there is more than one author, the order is up to you; the `\and` command provides for the separation.

Next the address(es) of institute(s), company etc. is (are) required. If there is more than one address, the entries are numbered automatically with `\and`, in the order in which you type them. Please make sure that the numbers match those placed next to to the authors' names to reflect the affiliation.

```
\institute{<name of an institute>
  \and <name of the next institute>
  \and <name of the next institute>}
```

If no institute is given, the LCIS address will be printed.

The number of the technical report (it is mandatory) should be provided as:

```
\TRnumber{<yy-nn(-v)>}
```

with the following format: `yy` = year, `nn` = number and `v` = version number (optional).

Also, some indexing terms (keywords) can be given. They will automatically be inserted after the abstract.

```
\keywords{<list of indexing terms>}
```

If footnote-like things are needed anywhere in the title heading please code (immediately after the word where the footnote indicator should be placed):

```
\thanks{<text>}
```

`\thanks` may only appear in `\title`, `\author` and `\institute` to footnote anything. If there are two or more footnotes or affiliation marks to a specific item separate them with `\fnmsep` (i.e. footnote mark separator).

3 Predefined Macros

The following macros are at your disposal:

Macro	Description
`\adLCIS`	LCIS address. This is useful to quickly encode the institute name of a LCIS member (see the examples).
`\LCIS`	LCIS logo. This macro is available is all sizes and shapes. Note that a space after "LCIS" can be forced by coding `\LCIS{}`.
`\qed`	□, usually to end a proof (Q.E.D.).

4 Predefined Theorem-like Environments

In addition to the above-mentioned macros, some theorem-like environments are predefined All the theorem-like environments are numbered automatically throughout the sections of your document. If your first call for such a theorem-like environment is `\begin{lemma}`, it will be numbered 1; if corollary follows, this will be numbered 2; if you then call lemma again, this will be numbered 3.

But in case you want to reset this counter to 1 in each section, please specify the documentclass option `envcountreset`:

```
\documentclass[envcountreset]{llncs}
```

Even a numbering on section level (including the section counter) is possible with the documentclass option `envcountsect`.

The following variety of run-in headings are at your disposal:

(a) **Bold** run-in headings with italicized text as built-in environments:

```
\begin{corollary} <text> \end{corollary}
\begin{lemma} <text> \end{lemma}
\begin{proposition} <text> \end{proposition}
\begin{theorem} <text> \end{theorem}
```

(b) The following generally appears as *italic* run-in heading:

```
\begin{proof} <text>    \qed    \end{proof}
```

It is unnumbered and may contain an eye catching square (call for that with `\qed`) before the environment ends.

(c) Further *italic* or **bold** run-in headings with roman environment body may also occur:

```
\begin{definition} <text> \end{definition}
\begin{example} <text> \end{example}
\begin{exercise} <text> \end{exercise}
\begin{note} <text> \end{note}
\begin{problem} <text> \end{problem}
\begin{question} <text> \end{question}
\begin{remark} <text> \end{remark}
\begin{solution} <text> \end{solution}
```

All these environments use and share by default one counter.

The syntax of the commands `\newtheorem` and `\newtheorem*` used to define additional environments has been changed. They now require two additional arguments namely the type style in which the keyword of the environment appears and second the style for the text of your new environment.

`\newtheorem` can be used in two ways:

Method 1 ***(preferred)*** You may want to create an environment sharing its counter with another environment, say `mainth` to be numbered like the predefined `theorem`. In this case, use the syntax

```
\newtheorem{<env_nam>}[<num_like>]{<caption>}{<cap_font>}{<body_font>}
```

Here the environment with which the new environment should share its counter is specified with the optional argument `[<num_like>]`.

Example:

```
\newtheorem{mainth}[theorem]{Main Theorem}{\bfseries}{\itshape}
```

The sharing of the default counter (`[theorem]`) is desired. If you omit the optional second argument of `\newtheorem` a separate counter for your new environment is used throughout your document.

Method 2 *(assumes* [envcountsect] *documentstyle option)*

```
\newtheorem{<env_nam>}{<caption>}[<within>]{<cap_font>}{<body_font>}
```

This defines a new environment <env_nam> which prints the caption <caption> in the font <cap_font> and the text itself in the font <body_font>. The environment is numbered beginning anew with every new sectioning element you specify with the optional parameter <within>.

Example:

```
\newtheorem{joke}{Joke}[subsection]{\bfseries}{\rmfamily}
```

defines a new environment called joke which prints the caption **Joke** in boldface and the text in roman. The jokes are numbered starting from 1 at the beginning of every subsection with the number of the subsection preceding the number of the joke e.g. 7.2.1 for the first joke in subsection 7.2.

If you wish to have an unnumbered environment, please use the syntax

```
\newtheorem*{<env_nam>}{<caption>}{<cap_font>}{<body_font>}
```

5 Examples

5.1 Single Authored Report

```
\documentclass[notitlepage]{lcistech}

\title{A New Cryptosystem}
\author{Marc Joye}
\institute{%
  \adLCIS\\
  Email: \texttt{joye@ee.tku.edu.tw}
}
\TRnumber{98-1}
\date{March 1, 1998}


\begin{document}

\maketitle

\begin{abstract}
  This report presents a new cryptosystem.
\end{abstract}

\section{Introduction}

  .
  .
  .

\section{Conclusion}
A new cryptosystem was proposed.

\end{document}
```

5.2 Multi-Authored Report

```
\documentclass{lcistech}

\title[An Ideal Cryptosystem]{An Ideal and Efficient Public-Key Cryptosystem
  Based on a non-NP Problem\thanks{Preliminary version, please do not redistribute.}
}
\author{Marc Joye\inst{1}\fnmsep\thanks{Supported by NSC under contract NSC-87-1234.}
  \and Jean-Jacques Quisquater\inst{2} \and Sung-Ming Yen\inst{1}
}
\institute{% address of institute 1 (M. Joye and S.-M. Yen)
    \adLCIS\\
    Email: \texttt{$\{$joye,yensm$\}$@ee.tku.edu.tw}
  \and % address of institute 2 (J.-J. Quisquater)
    UCL Crypto Group, Universit\'e de Louvain\\
    B-1348 Louvain-la-Neuve, Belgium\\
    Email: \texttt{quisquater@dice.ucl.ac.be}
}
\TRnumber{98-2-B}
\keywords{Public-key cryptography, Non-NP problems}
\date{April 1, 1998}


\begin{document}

\maketitle

\begin{abstract}
  This report presents an ideal and efficient public-key cryptosystem based on a non-NP problem.
\end{abstract}

\section{Introduction}

  .
  .
  .

\section{Conclusion}
An ideal and efficient public-key cryptosystem based on a non-NP problem was proposed.

\end{document}
```