

## Instructions for Authors of JMC

Robert Plato and Name of 2nd Author

Communicated by Communicating Editor

**Abstract.** Please provide an abstract. It should be self-contained, thus don't use references to the list of bibliography, and do not refer to specific theorems in the paper. This is important since after publication, abstracts will also be published online independently from the corresponding papers.

**Key words.** Key words; Example

**AMS classification.** 00X00, 00Y00

### 1 Introduction

These are instructions for authors to prepare a manuscript for the *Journal of Mathematical Cryptology*. Go to the subdirectory `template` and edit the file `main.tex`. This is the only file that has to be modified by authors.

### 2 Authors

Provide author information by using the commands `\authorx`, `\addressx`, `\countryx` and, if necessary, `\thanksx`. Here `x` can be one, two, three or four.

You may generate a short version for the author names in headlines by using the command `\headlineauthor`. Please provide keywords and an AMS 2000 Classification by the commands `\keywords` and `\classification`, respectively. If you want to include acknowledgments, please use the command `\acknowledgments`. All these commands have to be used in the preamble, i.e., they are to be placed before `\begin{document}`.

### 3 Your paper

In order to include your manuscript, you can make use of the `\input` command in the file `main.tex`, for example.

#### 3.1 Organizing your manuscript

You may use sections, subsections and subsubsections.

---

First author: Support of 1st author (optional).

Second author: Support of 2nd author (optional).

### 3.2 Styles

In titles of sections and subsections, please do not use words with capitalized first letters except for the first letter of the first word of the title as well as persons. Please notice that a blank line in  $\text{\TeX}$  ends a paragraph, and the subsequent line is indented. Equations are numbered as (1.1), (1.2), ..., (2.1) etc.

$$2 = 1 + 1. \quad (3.1)$$

In a definition, use italic fonts for the words to be defined.

**Definition 3.1.** An  $X$  satisfying  $Y$  is called *something*.

**Remark 3.2.** In addition to the **Definition** environment, several further environments for structuring the exposition are provided and can be accessed through commands like `\begin{algorithm}... \end{algorithm}`. The following environments are available:

- Algorithm, Assumption, Example, Remark and Proof, with the corresponding text bodies typeset in roman, respectively.
- Corollary, Lemma, Proposition and Theorem, with the corresponding text bodies typeset in italic, respectively.

### 3.3 Figures

Eps files may be included in the form

```
\begin{figure}[h]
  \centerline{\psfig{figure=xxx.eps,width=7cm} }
  \caption{\label{zzz}
    Text following the figure ....
  }
\end{figure}
```

## 4 Bibliography

For BibTeX users, a style file `wdg_jmc.bst` is provided. You have to add your databases in the command `\bibliography{}`. Running

```
latex main, bibtex main, latex main, latex main
```

will provide a file `main.dvi`. (In case you are using references within the bibliography, further executions of `bibtex main` and `latex main` may become necessary.) pdf files may be generated by the command `pdflatex`. Please do not use `dvips` to generate postscript files, it do not work properly due to the used packages.

Links to web sites (is useful for the online version of your paper) may be generated by the command `\href{link}{link}` where `link` refers to the web adress.

Here are a few entries from the sample database.bib in the sample directory.

```
@inproceedings{AARR,
author = {D. Agrawal and B. Archambeault and J. Rao and P. Rohatgi},
title = { The EM side-channel(s) },
booktitle = {Cryptographic Hardware and Embedded Systems -- CHES 2002},
series = {Lecture Notes in Computer Science},
number = {2523},
publisher = {Springer},
address = {Berlin, New York},
year = {2002},
pages = {29--45}}
```

```
@article{KM,
author = {N. Kobitz and A. Menezes},
title = {Another look at 'provable security'},
journal = {Journal of Cryptology, to appear},
note = {Available at \url{http://eprint.iacr.org/2004/152/}}
```

```
@article{NS,
author = { P. Nguyen and I. Shparlinski},
title = {The insecurity of the Digital Signature Algorithm
        with partially known nonces},
journal = {Journal of Cryptology},
volume = {15},
year = {2002},
pages = {151--176}}
```

```
@inproceedings{ko,
author = {E. Kushilevitz and R. Ostrovsky},
title = {Replication is not needed: single database, computationally
        private information retrieval},
booktitle = {Proceedings of the 38th IEEE Symposium on Foundations of
        Computer Science},
year = {1997},
pages = {364--373}}
```

```
@techreport{bfg,
author = {R. Beigel and L. Fortnow and W. Gasarch},
title = { A nearly tight lower bound for private information
        retrieval protocols},
institution = {Electronic Colloquium on Computational Complexity},
number = {87},
year = {2003}}
```

```
@book{Silv,
author = {J.~H.~Silverman},
title = {The Arithmetic of Elliptic Curves},
publisher = {Springer},
address = {Berlin, New York},
year = {1995}}
```

```
@phdthesis{TLdiss,
author = {T.~Lange},
title = {Efficient arithmetic on hyperelliptic curves},
school = {Universit\"at Gesamthochschule Essen},
year = {2001}}
```

```
@inproceedings{CLSQ,
author = {M.~Ciet and T.~Lange and F.~Sica and J.-J.~Quisquater},
```

---

```

title = {Improved algorithms for efficient arithmetic on elliptic
         curves using fast endomorphisms},
booktitle = {Advances in Cryptology -- Eurocrypt 2003},
series= {Lecture Notes in Computer Science},
number = 2656,
publisher = {Springer},
address = {Berlin, New York},
year = 2003,
pages = {388--400}}

@inproceedings{BlokhuisCHO,
author = {A.~Blokhuis and R.~S.~Coulter and M.~Henderson
and C.~M.~O'Keefe},
title = {Permutations amongst the {D}embowski-{O}strom polynomials},
booktitle = {Proceedings of The Fifth International Conference on
             Finite Fields and Applications - Fq5},
confaddress = {Augsburg},
confyear = {1999},
publisher = {Springer},
address = {Berlin, New York},
year = 2001}

@techreport{cryptoeprint2004143,
author = {N.~T.~Courtois},
title = {Short signatures, provable security, generic attacks and
         computational security of multivariate polynomial schemes
         such as {HFE}, {q}uartz and {s}flash},
institution = {Cryptology ePrint Archive},
number = {2004/143},
note = {Available at \url{http://eprint.iacr.org}}

@inproceedings{TC,
author = { T.~W.~Cusick },
title = {Boolean functions satisfying a higher order
         strict avalanche criterion},
booktitle = {Advances in Cryptology -- Eurocrypt '93},
pages = {102--117}}

@book{Finite,
author = { R.~Lidl and H.~Niederreiter},
title = {Finite Fields},
series = {Encyclopedia of Mathematics and Its Applications},
number = {20},
publisher = {Addison-Wesley},
address = {Reading, MA},
year = {1984}}

```

If you generate a bibliography without BibTeX, please use the same style as in the sample file provided in the sample subdirectory.

**Acknowledgments.** I would like to thank X, Y and Z for their valuable comments on earlier drafts of this paper

## References

- [1] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi, *The EM side-channel(s)*. Cryptographic Hardware and Embedded Systems – CHES 2002, Lecture Notes in Computer Science 2523, pp. 29–45. Springer, Berlin, New York, 2002.
- [2] R. Beigel, L. Fortnow, and W. Gasarch, *A nearly tight lower bound for private information retrieval protocols*, Electronic Colloquium on Computational Complexity, Report no. 87, 2003.
- [3] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O’Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*. Proceedings of The Fifth International Conference on Finite Fields and Applications - Fq5 (Augsburg 1999). Springer, Berlin, New York, 2001.
- [4] M. Ciet, T. Lange, F. Sica, and J.-J. Quisquater, *Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms*. Advances in Cryptology – Eurocrypt 2003, Lecture Notes in Computer Science 2656, pp. 388–400. Springer, Berlin, New York, 2003.
- [5] N. T. Courtois, *Short signatures, provable security, generic attacks and computational security of multivariate polynomial schemes such as HFE, quartz and sflash*, Cryptology ePrint Archive, Report no. 2004/143. Available at <http://eprint.iacr.org>.
- [6] T. W. Cusick, *Boolean functions satisfying a higher order strict avalanche criterion*. Advances in Cryptology – Eurocrypt ’93, pp. 102–117.
- [7] N. Kobitz and A. Menezes, *Another look at ‘provable security’*, Journal of Cryptology, to appear. Available at <http://eprint.iacr.org/2004/152/>.
- [8] E. Kushilevitz and R. Ostrovsky, *Replication is not needed: single database, computationally private information retrieval*. Proceedings of the 38th IEEE Symposium on Foundations of Computer Science, pp. 364–373, 1997.
- [9] T. Lange, *Efficient arithmetic on hyperelliptic curves*, Ph.D. thesis, Universität Gesamthochschule Essen, 2001.
- [10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications 20. Addison-Wesley, Reading, MA, 1984.
- [11] P. Nguyen and I. Shparlinski, *The insecurity of the Digital Signature Algorithm with partially known nonces*, Journal of Cryptology 15 (2002), pp. 151–176.
- [12] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Springer, Berlin, New York, 1995.

Received 12 January, 2007; revised 13 January, 2007

## Author information

Robert Plato, Walter de Gruyter, Berlin/New York, Germany/USA.  
Email: [author1@affiliati.on1](mailto:author1@affiliati.on1)

Name of 2nd Author, affiliation and address of 2nd author, country of 2nd author.  
Email: [author2@affiliati.on2](mailto:author2@affiliati.on2)