DE GRUYTER

Last update: August 1, 2022

# Instructions for Authors

## Scope

*Journal of Mathematical Cryptology (JMC)* is a fully peer-reviewed, open access, electronic journal that publishes significant, original and relevant works in all areas of mathematics. The scope includes mathematical results of algorithmic or computational nature that are of interest to cryptology.

### Topics

- Mathematical cryptology
- Information security
- Theory of cryptology
- Quantum cryptology
- Algebra
- Algebraic geometry
- Coding theory
- Combinatorics and Graph Theory
- Number theory
- Probability and stochastic processes
- theory of cryptology
- work linking math to cryptology
- work in the mathematical foundations of crypto

Articles accepted for publication in the Journal of Mathematical Cryptology are subject to Article Processing Charges (APCs). The publication fee amounts to 1000 EUR. **Authors who have no funding for the submitted research can request a waiver or a discount during the submission process**. For more details please check Article Processing Charges.

## Editorial Policy

### Unpublished material

Submission of a manuscript implies that the work described is not copyrighted, published or submitted elsewhere, except in abstract form. The corresponding author should ensure that all authors approve the manuscript before its submission.

### Conflict of interest

When authors submit a manuscript, they are responsible for recognizing and disclosing financial and/or other conflicts of interest that might bias their work and/or could inappropriately influence his/her judgment. If no specified acknowledgement is given, the Editors assume that no conflict of interest exists.

### Copyright



### Authorship

Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as coauthors. Where there are others who have participated in certain substantive aspects of the research project, they should be named in an Acknowledgement section.

### Peer Review process

The Editors reserve the right to decline the submitted manuscript without review, if the studies reported are not sufficiently novel or important to merit publication in the journal. Manuscripts deemed unsuitable (insufficient originality or of limited interest to the target audience) are returned to the author(s) without review. The Editor seeks advice from experts in the appropriate field. Research articles and communications are refereed by a minimum of two reviewers, review papers by at least three. The journal uses single-blind peer review model. Authors are requested to suggest persons competent to review their manuscript. However, please note that this will be treated only as a suggestion, and the final selection of reviewers is exclusively the Editor's decision. The final decision of acceptance is made by the Editors-in-Chiefs of the journal.

### Data sharing policy

Effective December 2020, the journal requires authors to follow data sharing policy. Research data should be made widely available to the research community in order to demonstrate the robustness and validity of the research presented in the journal, to encourage replication of the results, and to provide the community with opportunities to learn. By publishing in the journal authors are required to provide a data availability statement (DAS) in their articles. Authors are encouraged to share their data but not required to. The decision to publish will not be affected by whether or not authors share their research data.

### Scientific Misconduct

This journal publishes only original manuscripts that are not also published or going to be published elsewhere. Multiple submissions/publications, or redundant publications (re-packaging in different words of data already published by the same authors) will be rejected. If they are detected only after publication, the journal reserves the right to publish a Retraction Note. In each particular case Editors will follow COPE's Code of Conduct and implement its advice.

## Electronic Submission

*Journal of Mathematical Cryptology* encourages the submission of both substantial full-length bodies of work and shorter manuscripts that report novel findings. There are no specific length restrictions for the overall manuscript or individual sections; however, we urge the authors to

present and discuss their findings in a concise and accessible manner. All submitted manuscripts must be written in English language. It is the Authors' responsibility to check the correctness of the language and style of their manuscript.

Manuscripts submitted under multiple authorship are reviewed on the assumption that all listed authors concur in the submission and are responsible for its content; they must have agreed to its publication and have given the corresponding author the authority to act on their behalf in all matters pertaining to publication. The corresponding author is responsible for informing the coauthors of the manuscript status throughout the submission, review, and production process.
All manuscripts must be made electronically via ScholarOne, an online submission and peer review system (http://mc.manuscriptcentral.com/jmc). First-time users must create an Author account in order to obtain a user ID and password required to enter the system. All manuscripts receive individual identification codes that should be used in any correspondence with regard to the publication process. If you experience difficulties with the manuscript submission website, please contact the Editorial Office - jmc_Editorial@degruyter.com

## Publication Formats

*Journal of Mathematical Cryptology* considers submissions of:

- Research Article – The default format for reporting research results. There is no length restriction.
- Review Article – Used to submit literature reviews on a topic of interest. The article should contain a broad, balanced and fair perspective of the topic, identifying trends and/or gaps in the literature or providing a new synthesis of existing literature. Reviews should be scientifically sound and should describe the most relevant and recent contributions.
- Mini-Review Article – A shorter form of a Review Article intended for a brief analysis of a focused topic on advances in the field. It discusses recent experimental research, highlights recent developments in fastmoving areas and suggests areas that require additional research.
- Communication – This format is intended for the presentation of brief observations that do not warrant fulllength papers. An empirical report resulting from analysis of collected data to address one or more research questions and/or hypotheses

### Electronic Formats Allowed

We accept submission of text, tables and figures as separate files or as a composite file. For your initial submission, we recommend you upload your entire manuscript, including tables and figures, as a single PDF file. If you are invited to submit a revised manuscript, please provide us with individual files: an editable text and publication-quality figures.

- Text files can be submitted in the following formats:
  - LATEX, AMS-TEX, AMS-LATEX. We do not accept papers in Plain TEX format. Authors are strongly advised to submit the final version of the paper using the journal's LATEX template.
  - MS Word - standard DOCUMENT (.DOC) or RICH TEXT FORMAT (.RTF) are also acceptable.

- Tables should be embedded in LATEX (strongly preferred) or submitted as PDF (not applicable for accepted manuscripts, only for reviewing process). Please note that a straight Excel file is not an acceptable format.
- Graphics files can be submitted in any of the following graphic formats: EPS; BMP; JPG; TIFF; GIF or PDF. Please note that Powerpoint files are not accepted.

Post-acceptance, text files of the revised manuscript and tables are required for use in the production. Authors should clearly indicate the location(s) of tables and figures in the text if these elements are given separately or at the end of the manuscript. If this information is not provided to the editorial office, we will assume that they should be left at the end of the text.

## First-Time Submission of Manuscripts

It is important that authors include a cover letter with their manuscript. Please explain why you consider your manuscript to be suitable for publication in *Journal of Mathematical Cryptology*, why your paper will inspire the other members of your field, and how will it drive academic discussion forward.

The cover letter should explicitly state that the manuscript (or one with substantially the same content, by any of the authors) has not been previously published in any language anywhere and that it is not under simultaneous consideration or in press by another journal. If related work has been submitted, then we may require a preprint to be made available. Reviewers will be asked to comment on the overlap between the related submissions.

Manuscripts that have been previously rejected, or withdrawn after being returned for modification, may be resubmitted if the major criticisms have been addressed. The cover letter must state that the manuscript is a resubmission, and the former manuscript number should be provided.

To ensure fair and objective decision-making, authors must declare any associations that pose a conflict of interest in connection with evaluated manuscripts. Authors may suggest up to two referees not to use, and in such cases additional justification should be provided in the cover letter. Authors are encouraged to recommend up to five reviewers who are not members of their institution(s) and have never been associated with them or their laboratory(ies); please provide contact information for suggested reviewers. The Editors reserve the right to select expert reviewers at their discretion.

## Submission of Revised Articles

Resubmitted manuscripts should be accompanied by a letter outlining a point-by-point response to Editor's and reviewers' comments and detailing the changes made to the manuscript. A copy of the original manuscript should be included for comparison if the Editor requests one. If it is the first revision, authors need to return the revised manuscript within 28 days; if it is the second revision, authors need to return the revised manuscript within 14 days. Additional time for resubmission must be requested in advance. If the above-mentioned deadlines are not met, the manuscript will be treated as a new submission.

For resubmitted manuscripts, please provide us with an editable text and publication-quality figures. Supply any figures as separate high-resolution, print-ready digital versions. In addition to the editorial remarks, authors are asked to take care that they have prepared the revised version according to the Journal's style.

## Organization of the Manuscript

We draw particular attention to the importance of carefully preparing the title, keywords and abstract, as these elements are indicators of the manuscript content in bibliographic databases and search engines.

### Title

We suggest the title should be informative, specific to the project, yet concise (75 characters or fewer). If a long title is necessary, please prepare an optional short title. Please bear in mind that a title that is comprehensible to a broad academic audience and readers outside your field will attract a wider readership. Avoid specialist abbreviations and non-standard acronyms. Titles should not be presented in title case (words should not be capitalized).

### Authors, Affiliations, Addresses

In the cover letter, provide the first names (or initials – if used), middle names (or initials – if used), and surnames for all authors. Affiliations should include:

- Department
- University or organization
- City
- Postal code
- State/province (if applicable)
- Country

One of the authors should be designated as the corresponding author to whom inquiries regarding the paper should be directed. It is the corresponding author's responsibility to ensure that the author list and the summary of the author contributions to the study are accurate and complete.

### Abstract

The abstract should not exceed 200 words. The abstract should give a summary of the content of the paper. Mention the main findings without going into methodological detail and summarize briefly the most important items of the paper. The abstract should not contain literature citations, allusions to the tables, tables, figures or illustrations. All nonstandard symbols and abbreviations should be defined. In combination with the title and keywords, an abstract is an indicator of the content of the paper. Because the abstract will be published separately by abstracting services, it must be complete and understandable without reference to the text.

## Classification numbers

Please include AMS Mathematics Subject Classification number(s) to which the paper can be attributed. More than a single classification number may be accepted. For AMS Mathematics Subject Classification (MSC 2020) see https://mathscinet.ams.org/msc/msc2020.html

## Keywords

List keywords for the work presented (maximum of 6), separated by commas. We suggest that keywords do not replicate those used in the title.

## Structure of a paper

Research papers and surveys should follow a strict structure. Generally, a standard scientific paper is divided into:

- introduction: present the subject of your paper clearly, indicate the scope of the subject, present the goals of your paper and finally the organization of your paper;
- main text: present all important elements of your scientific message;
- conclusion: summarize your paper.

The journal is published in English. Make sure that your manuscript is clearly and grammatically written. It is the Authors' responsibility to ensure the language of their manuscript is correct. This should be preferably done prior to submission and we recommend the verification of the language with a native speaker. The mathematical content should be understandable and should not cause any confusion to the readers, including the referees.

General rules for writing:

- use simple and declarative sentences, avoid long sentences, in which the meaning may be lost by complicated construction;
- use correct and established nomenclature whenever possible;
- make your argumentation complete; use commonly understood terms; define all nonstandard symbols and abbreviations when you introduce them;
- explain all acronyms and abbreviations when they first appear in the text;
- use all units consistently throughout the article;
- be self-critical as you review your drafts.

## Footnotes/Endnotes

We encourage authors to restrict the use of footnotes. If necessary, please make endnotes rather than footnotes.

A footnote/endnote may include:

- the designation of the corresponding author of the paper;
- the current address of an author (if different from that shown in the affiliation);
- traditional footnote content.

Information concerning research grant support should appear in a separate Funding Information section at the end of the paper, not in a footnote. Acknowledgements of the assistance of

colleagues or similar notes of appreciation should also appear in the Acknowledgements section, not in footnotes.

## Acknowledgments

This section should describe recognition of personal assistance: people who contributed to the work, but do not fit the criteria for authors should be listed along with their contributions. You must ensure that anyone named in the acknowledgments agrees to being so named.

## Author's Statements

This section should describe:

- any funding information, including the role of the study sponsor(s), if any, in study design, collection, analysis, and interpretation of data, writing the paper and decision to submit it for publication;
- authors contribution -if required;
- conflict of interest;
- Data Availability Statement (if applicable).

Please refer to Author's Statement document.

## References

Because all references will be linked electronically to the papers they cite, proper formatting of the references is crucial. A complete reference should give the reader enough information to find the relevant article. Please pay particular attention to spelling, capitalization and punctuation.

Abbreviated journals names should be written according to Mathematical Reviews Serials Abbreviations, see http://www.ams.org/msnhtml/serials.pdf

References to unpublished or submitted work, unpublished conference presentations, personal communications, patent applications and patents pending, computer software, databases, and websites should be referred to as such only in the body of the text. These should be kept to a minimum.

References should be listed and numbered in the order that they appear in the text. In the text, citations should be indicated by the reference number in brackets [1]. Multiple citations within a single set of brackets should be separated by commas [1, 5]. Where there are more than three sequential citations, they should be given as a range [1-4]. References in figure captions and tables should be listed after the references in the text.

Please use the **Vancouver** style for the reference list:

Published papers

Kurdachenko L.A., Semko N.N., Subbotin I.Ya. The Leibniz algebras whose subalgebras are ideals. *Open Math*. 2017;15(1): 92–100. Available from: https://doi.org/10.1515/math-2017-0010

Accepted papers

Kurdachenko L.A., Semko N.N., Subbotin I.Ya. The Leibniz algebras whose subalgebras are ideals. *Open Math*.

Electronic journal articles

Dionne M.S., Schneider D.S. Screening the immune system. Genome Biology, http://genomebiology.com/2002/3/4/reviews/1010.

Books and book chapters

Gigli N. (Ed.). *Measure Theory in Non-Smooth Spaces*. De Gruyter Publishing Group; 2017

Bogachev V.I. Surface measures in infinite-dimensional spaces. In: Gigli N. (Ed.) *Measure Theory in Non-Smooth Spaces*. De Gruyter Publishing Group; 2017. p. 52-97

Sambrook, J., Russell D.W., *Molecular cloning - a laboratory manual (3rd ed.)*. New York: Cold Spring Harbor Laboratory Press; 2001

Theses

Agutter A.J., Analysis of sigma factors in S. aureus (PhD thesis). Edinburgh: Edinburgh University; 1995

Conference proceedings

Smith J., Brown P., Reference style guide, In: Scott M. (Ed.). *Proceedings of Biochemical Society Conference, 11-13 July 2007, Warsaw, Poland*. Warsaw: Versita; 2007. p. 1335-1791.

Newspaper articles

Sherwin A., The post-genomic era. The Times. 2007 Jul 16:170 (3), 1-2.

Dzierzanowski M. Horyzonty. Wprost. 2007 Jul 8:18 (in Polish).

## Formatting and Typesetting

All pages must be numbered consecutively. The whole text (including legends, footnotes, and references) should be formatted no hyphenation and automatic word-wrap (no hard returns within paragraphs). Please type your text consistently, e.g. take care to distinguish between '1' (one), 'l' (capital I) and 'l' (lower-case L) and '0' (zero) and 'O' (capital O), etc. Manuscript pages should have line numbers. The font size should be no smaller than 12 points.

Footnotes and endnotes should be avoided. Allowable footnotes/endnotes may include: the designation of the corresponding author of the paper, the current address of an author (if different from that shown in the affiliation), abbreviations and acronyms.

## Figures and Figure Legends

Authors may use photographs, schemes, diagrams, line graphs and bar charts to illustrate their findings, Figures should be suitable for onscreen viewing and desktop printing. High resolution images should be provided on request or on manuscript acceptance. The figures and their lettering should be clear and easy to read.

We remind the authors that it is not acceptable scientific conduct to modify any separate element within an image. Figures should be numbered consecutively using Arabic numerals and referred to in the text by number. Each figure legend should have a concise title and should provide enough information so that the figure is understandable without frequent reference to the text.

## Tables and Table Captions

Tables must include enough information to warrant table format and should be used only where information cannot be presented in the text. Please do not use graphics software to create tables. Tables occupying more than one printed page should be avoided, if possible; larger tables can be published as an appendix. Tables should be numbered consecutively using Arabic numerals and

referred to in the text by number. Each table should have an explanatory caption which should be as concise as possible. The headings should be sufficiently clear so that the meaning of the data is understandable without reference to the text. Any citations should be indicated using the same style as above.

### Symbols and abbreviations

The use of special symbols, abbreviations, and acronyms is permitted so long as they are defined upon first mention in the article.

### Supplemental Material

We encourage authors to submit essential supplementary files that additionally support the authors' conclusions with their manuscripts (the principal conclusions should be fully supported without referral to the supplemental material). Supplemental material will always remain associated with its article and is not subject to any modifications after publication. The decision to publish the material with the article if it is accepted will be made by the Editor. Supporting files of no more than 10 MB in size may be submitted in a variety of formats, but should be publication-ready, as the files will be published exactly as supplied. Material must be restricted to large or complex data sets or results that cannot be readily displayed because of space or technical limitations. Material that has been published previously is not acceptable for posting as supplemental material.

Supporting files should fall into one of the following categories:

- Dataset
- Additional Figure or Table
- Text
- Protocol
- Multimedia – Audio/Video/Animations (AVI, MPEG, WAV, Quicktime, animated GIF or Flash)

If the software requires for uses to view/use the supplemental material is not embedded in the file, you are urged to use shareware or generally available/easily accessible programs. To prevent any misunderstanding, we request that authors submit a text file (instruction.txt) containing a brief instruction on how to use the files supplied.

## Outline of the Production Process

Once an article has been accepted for publication, the manuscript files are transferred into our production system to be formatted. At this stage, it is assumed that the language of the manuscript has been checked for correctness and style. If not, the Authors are asked to verify the language before sending the final source files (we recommend verification by a native speaker). Technical editors reserve the privilege of editing manuscripts to conform with the stylistic conventions of the journal. Once the article has been typeset, PDF proofs are generated so that authors can approve all editing and layout.

## Electronic Proofs

Proofreading should be carried out once a final draft has been produced. Since the proofreading stage is the last opportunity to correct the article to be published, the authors are requested to make every effort to check for errors in their proofs before the paper is posted online. Please note that only essential changes can be made at this stage and extensive corrections, additions, or deletions will not be allowed. Limit changes to correction of spelling errors, incorrect data, grammatical errors, and updated information for references to articles that have been submitted or are in press. If URLs have been provided in the article, recheck the sites to ensure that the addresses are still accurate and the material that you expect the reader to find is indeed there. Important new information that has become available between acceptance of the manuscript and receipt of the proofs may be inserted into the proof with the permission of the editor.

Additionally, authors may be asked to address remarks and queries from the technical editors. Queries are written only to request necessary information or clarification of an unclear passage or to draw attention to edits that may have altered the sense. Please note that technical editors do not query at every instance where a change has been made. It is the author's responsibility to read the entire text, tables, and figure legends, not just items queried. Major alterations made will always be submitted to the authors for approval.

Manuscripts submitted under multiple authorship are published on the assumption that the final version of the manuscript has been seen and approved by all authors. The Corresponding author will receive e-mail notification when a downloadable PDF file is available and should return comments on the proofs within a maximum of 3 days of receipt. Comments should be e-mailed to Journal Editor. Please note that they should not be faxed, nor mailed or sent by a courier service to the Editorial Office.

## Immediate Publication

Manuscripts ready for publication are promptly posted online. The manuscripts are considered to be ready for publication when the final proofreading has been performed by authors, and all concerns have been resolved. Authors should notice that no changes can be made to the articles after online publication.