[[1]](#footnote-1)

Significantly Improving the Homomorphic Secret Sharing Scheme in the Voter Model

Ben Jones, Ethan Mines, Philip Speegle

*Abstract*—These instructions give you guidelines for preparing papers for IEEE TRANSACTIONS and JOURNALS*.* Use this document as a template if you are using Microsoft *Word* 6.0 or later. Otherwise, use this document as an instruction set. The electronic file of your paper will be formatted further at IEEE. Define all symbols used in the abstract. Do not cite references in the abstract. Do not delete the blank line immediately above the abstract; it sets the footnote at the bottom of this column.

# INTRODUCTION

I

n this paper, we implement improvements to Homomorphic Secret Sharing (HSS) schemes to secure voting. HSS Schemes were first introduced in 2016 by [1]. We begin with a high-level comparison of HSS schemes with their predecessors, Fully Homomorphic Encryption (FHE) and Function Secret Sharing (FSS). This comparison provides clarity and context that highlight the benefits that HSS provides in relation to the others. In particular, we consider the improvements that [2] make to existing HSS schemes, and apply them to voting. We construct an implementation of the ElGamal cryptosystem, which will be used as a major basis element in the implementation of the HSS algorithms.

## Homomorphic Encryption

Homomorphic encryption allows a user to perform operations on encrypted data without decrypting it [3]. An example use case of this is secure cloud computation. With homomorphic encryption, Alice could encrypt her financial data and upload it to a remote server, owned by Bob. Bob could then sum the numbers in the financial data, without knowledge of what the numbers are. Bob then sends back the encrypted result, which is finally decrypted by Alice. In this case, Alice is the only entity that knows the plaintext, but Alice was able to outsource her computation to Bob.

In [3], Gentry categorizes homomorphic encryption schemes into several classes. Two examples of these are the partially homomorphic and fully homomorphic. In a partially homomorphic cryptosystem, the user is able to perform precisely one operation on the encrypted data, such as addition or multiplication. In contrast, fully homomorphic encryption (FHE) allows the user to do arbitrary computation. In 2009 and after being an open problem since 1978, Craig Gentry proposed the first viable FHE scheme in [3].

One way to formalize the concept of FHE is to create a scheme ℰ with an algorithm Eval that can evaluate an arbitrary logical circuit C, with algorithms Encrypt and Decrypt for encrypting data and decrypting it, respectively. Gentry accomplished this with a concept called “bootstrapping.” A scheme ℰ is bootstrappable whenever the evaluation algorithm can compute the decryption algorithm Decrypt and an augmented NAND gate. From this, Gentry proves that you can create a complete set of circuits [3]. Finally, he constructs a bootstrappable scheme.

## Function Secret Sharing

This subsection summarizes the seminal paper on function secret sharing in a format that will be used to compare FSS to HSS. The full details can be found in [4].

A function secret sharing scheme splits a function into secure "shares" such that certain subsets of the shares cannot be recombined to give an advantage in computing the original function.

More precisely, an FSS scheme has 6 components. The first is a set of p parties, denoted [p] who will receive the shares. The second is a subset T of [p] that are adversaries. The third is a class of functions, ℱ, containing our eventually secret function. The fourth is an output decoder algorithm, Dec, that takes the shares as inputs and decodes it as a single output. This is usually a sum function. The fifth is a key generation algorithm Gen that generates the p “keys” or “shares” for the input function, according to a security parameter constraint. The sixth and final component is an evaluation function, Eval, that evaluates each function share.

The FSS is also subject to a correctness and security constraint. The correctness constraint rigorously states that with probability 1, the decoder algorithm operating on the shares generated from a function, f, will return the same value as f. The security constraint for

## Overview of Homomorphic Secret Sharing

Homomorphic secret sharing was originally conceived as a dual to function secret sharing, which splits the *program* rather than the inputs into shares [4],[1].

Of the variants of homomorphic secret sharing described in [1], we use *Distributed Evaluation Homomorphic Encryption*, which allows multiple clients to send shares of inputs to two servers [1],[2].

During computations by the servers, multiplicative shares of a program variable must sometimes by converted to additive ones [2].

This is done via a probabilistic procedure known as DistributedDLog that relies on a pseudorandom function.

If each of the two servers call the procedure on their multiplicative share , they each receive a new additive share such that .

Since this is a probabilistic procedure, the outputs fail to be correct additive shares with probability at most , where is a parameter that can tweaked such that lower values of result in longer runtimes of the procedure.

This is the primary limiting factor of the size of programs executed by the servers: error may accumulate by repeated calls to DistributedDLogn [1].

# Simple ElGamal Cryptosystem

The ElGamal cryptosystem is an asymmetric cryptosystem making use of a public key and a single-use private or `ephemeral key.'

One of its variants is homomorphic with respect to addition, making it a suitable candidate for Homomorphic Secret Sharing.

## Key Generation and Encryption

Consider a voting system where there are questions and two options for each question, {0,1}. Let denote the set of all possible permutations of options chosen given that all the questions were answered. Then, we define the bijective map which maps each coefficient of to the chosen option for question . Note that this bijection implies that there are possible outcomes for a vote. For a quick example, let . Then, the eight possible outcomes are . It will be advantageous to utilize the fact that all elements of can be written in binary by only using their coefficients. As such, we seek a group order such that .

Let be a cyclic group of order , where and are primes. Recall that , and the amount of generators of is , where each element in is all for which . Then, the proposed generation algorithm is as follows. First, we randomly generate two distinct prime numbers and , preferably making the product large. Using the Miller-Rabin primality test, large values of primes can be found easily. Without loss of generality, assume . Compute and let . Randomly choose an integer until is sufficient such that $. The following results show that, for sufficiently large and , the time this takes is essentially negligible.

**Proposition II.1.** Let .Then,

where is Euler’s Totient function.

*Proof.* It is well-known that is a multiplicative homomorphism, so we have . The primality of both and implies and , and the result trivially follows.□

**Remark:** Indeed, is quite close to itself. This notion is rigorized in the following theorem:

**Theorem II.1.** Let where for two distinct primes . Then, with probability.

*Proof.* Consider . Since and are both prime, . For all integers . So the amount of possible generators for is surely since we require We sample a total of elements, so the probability of choosing a generator is , as desired.□

se it to prepare your manuscript. If you would prefer to use LATEX, download IEEE’s LATEX style and sample files from the same Web page. Use these LATEX files for formatting, but please follow the instructions in TRANS-JOUR.DOC or TRANS-JOUR.PDF.

If your paper is intended for a *conference,* please contact your conference editor concerning acceptable word processor formats for your particular conference.

When you open TRANS-JOUR.DOC, select “Page Layout” from the “View” menu in the menu bar (View | Page Layout), which allows you to see the footnotes. Then type over sections of TRANS-JOUR.DOC or cut and paste from another document and then use markup styles. The pull-down style menu is at the left of the Formatting Toolbar at the top of your *Word* window (for example, the style at this point in the document is “Text”). Highlight a section that you want to designate with a certain style, then select the appropriate name on the style menu. The style will adjust your fonts and line spacing. **Do not change the font sizes or line spacing to squeeze more text into a limited number of pages.** Use italics for emphasis; do not underline.

To insert images in *Word,* position the cursor at the insertion point and either use Insert | Picture | From File or copy the image to the Windows clipboard and then Edit | Paste Special | Picture (with “Float over text” unchecked).

IEEE will do the final formatting of your paper. If your paper is intended for a conference, please observe the conference page limits.

# Procedure for Paper Submission

## Review Stage

Please check with your editor on whether to submit your manuscript by hard copy or electronically for review. If hard copy, submit photocopies such that only one column appears per page. This will give your referees plenty of room to write comments. Send the number of copies specified by your editor (typically four). If submitted electronically, find out if your editor prefers submissions on disk or as e-mail attachments.

If you want to submit your file with one column electronically, please do the following:

--First, click on the View menu and choose Print Layout.

--Second, place your cursor in the first paragraph. Go to the Format menu, choose Columns, choose one column Layout, and choose “apply to whole document” from the dropdown menu.

--Third, click and drag the right margin bar to just over 4 inches in width.

The graphics will stay in the “second” column, but you can drag them to the first column. Make the graphic wider to push out any text that may try to fill in next to the graphic.

## Final Stage

When you submit your final version, after your paper has been accepted, print it in two-column format, including figures and tables. Send three prints of the paper; two will go to IEEE and one will be retained by the Editor-in-Chief or conference publications chair.

You must also send your final manuscript on a disk, which IEEE will use to prepare your paper for publication. Write the authors’ names on the disk label. If you are using a Macintosh, please save your file on a PC formatted disk, if possible. You may use *Zip* or CD-ROM disks for large files, or compress files using *Compress, Pkzip, Stuffit,* or *Gzip.*

Also send a sheet of paper with complete contact information for all authors. Include full mailing addresses, telephone numbers, fax numbers, and e-mail addresses. This information will be used to send each author a complimentary copy of the journal in which the paper appears. In addition, designate one author as the “corresponding author.” This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

## Figures

All tables and figures will be processed as images. **However, IEEE cannot extract the tables and figures embedded in your document.** (The figures and tables you insert in your document are only to help you gauge the size of your paper, for the convenience of the referees, and to make it easy for you to distribute preprints.) Therefore, **submit, on separate sheets of paper, enlarged versions of the tables and figures that appear in your document.** These are the images IEEE will scan and publish with your paper.

## Electronic Image Files (Optional)

You will have the greatest control over the appearance of your figures if you are able to prepare electronic image files. If you do not have the required computer skills, just submit paper prints as described above and skip this section.

*1) Easiest Way:* If you have a scanner, the best and quickest way to prepare noncolor figure files is to print your tables and figures on paper exactly as you want them to appear, scan them, and then save them to a file in PostScript (PS) or Encapsulated PostScript (EPS) formats. Use a separate file for each image. File names should be of the form “fig1.ps” or “fig2.eps.”

*2) Slightly Harder Way:* Using a scanner as above, save the images in TIFF format. High-contrast line figures and tables should be prepared with 600 dpi resolution and saved with no compression, 1 bit per pixel (monochrome), with file names of the form “fig3.tif” or “table1.tif.” To obtain a 3.45-in figure (one-column width) at 600 dpi, the figure requires a horizontal size of 2070 pixels. Typical file sizes will be on the order of 0.5 MB.

Photographs and grayscale figures should be prepared with 220 dpi resolution and saved with no compression, 8 bits per pixel (grayscale). To obtain a 3.45-in figure (one-column width) at 220 dpi, the figure should have a horizontal size of 759 pixels.

Color figures should be prepared with 400 dpi resolution and saved with no compression, 8 bits per pixel (palette or 256 color). To obtain a 3.45-in figure (one column width) at 400 dpi, the figure should have a horizontal size of 1380 pixels.

For more information on TIFF files, please go to <http://www.ieee.org/organizations/pubs/transactions/information.htm> and click on the link “Guidelines for Author Supplied Electronic Text and Graphics.”

*3) Somewhat Harder Way:* If you do not have a scanner, you may create noncolor PostScript figures by “printing” them to files. First, download a PostScript printer driver from <http://www.adobe.com/support/downloads/pdrvwin.htm> (for Windows) or from [http://www.adobe.com/support/downloads/ pdrvmac.htm](http://www.adobe.com/support/downloads/) (for Macintosh) and install the “Generic PostScript Printer” definition. In *Word,* paste your figure into a new document. Print to a file using the PostScript printer driver. File names should be of the form “fig5.ps.” Use Adobe Type 1 fonts when creating your figures, if possible.

*4) Other Ways:* Experienced computer users can convert figures and tables from their original format to TIFF. Some useful image converters are Adobe *Photoshop,* Corel *Draw,* and Microsoft *Photo Editor,* an application that is part of Microsoft *Office 97* and *Office 2000* (look for C:\Program Files\Common Files \Microsoft Shared\ PhotoEd\ PHOTOED.EXE. (You may have to custom-install *Photo Editor* from your original *Office* disk.)

Here is a way to make TIFF image files of tables*.* First, create your table in *Word.* Use horizontal lines but no vertical lines. Hide gridlines (Table | Hide Gridlines). Spell check the table to remove any red underlines that indicate spelling errors. Adjust magnification (View | Zoom) such that you can view the entire table *at maximum area* when you select View | Full Screen. Move the cursor so that it is out of the way. Press “Print Screen” on your keyboard; this copies the screen image to the Windows clipboard. Open Microsoft *Photo Editor* and click Edit | Paste as New Image. Crop the table image (click Select button; select the part you want, then Image | Crop). Adjust the properties of the image (File | Properties) to monochrome (1 bit) and 600 pixels per inch. Resize the image (Image | Resize) to a width of 3.45 inches. Save the file (File | Save As) in TIFF with no compression (click “More” button).

Most graphing programs allow you to save graphs in TIFF; however, you often have no control over compression or number of bits per pixel. You should open these image files in a program such as Microsoft *Photo Editor* and re-save them using no compression, either 1 or 8 bits, and either 600 or 220 dpi resolution (File | Properties; Image | Resize). See Section II-D2 for an explanation of number of bits and resolution. If your graphing program cannot export to TIFF, you can use the same technique described for tables in the previous paragraph.

A way to convert a figure from Windows Metafile (WMF) to TIFF is to paste it into Microsoft *PowerPoint,* save it in JPG format, open it with Microsoft *Photo Editor* or similar converter, and re-save it as TIFF.

Microsoft *Excel* allows you to save spreadsheet charts in Graphics Interchange Format (GIF). To get good resolution, make the *Excel* charts *very* large. Then use the “Save as

HTML” feature (see [http://support.microsoft.com/support/ kb/articles/q158/0/79.asp](http://support.microsoft.com/support/)). You can then convert from GIF to TIFF using Microsoft *Photo Editor,* for example.



Fig. 1. Magnetization as a function of applied field. Note that “Fig.” is abbreviated. There is a period after the figure number, followed by two spaces. It is good practice to explain the significance of the figure in the caption.

No matter how you convert your images, it is a good idea to print the TIFF files to make sure nothing was lost in the conversion.

If you modify this document for use with other IEEE journals or conferences, you should save it as type “Word 97-2000 & 6.0/95 - RTF (\*.doc)” so that it can be opened by any version of *Word.*

## Copyright Form

TABLE I

Units for Magnetic Properties

|  |  |  |
| --- | --- | --- |
| Symbol | Quantity | Conversion from Gaussian and  CGS EMU to SI a |
| Φ | magnetic flux | 1 Mx → 10−8 Wb = 10−8 V·s |
| *B* | magnetic flux density,  magnetic induction | 1 G → 10−4 T = 10−4 Wb/m2 |
| *H* | magnetic field strength | 1 Oe → 103/(4π) A/m |
| *m* | magnetic moment | 1 erg/G = 1 emu  → 10−3 A·m2 = 10−3 J/T |
| *M* | magnetization | 1 erg/(G·cm3) = 1 emu/cm3  → 103 A/m |
| 4π*M* | magnetization | 1 G → 103/(4π) A/m |
| σ | specific magnetization | 1 erg/(G·g) = 1 emu/g → 1 A·m2/kg |
| *j* | magnetic dipole  moment | 1 erg/G = 1 emu  → 4π × 10−10 Wb·m |
| *J* | magnetic polarization | 1 erg/(G·cm3) = 1 emu/cm3  → 4π × 10−4 T |
| χ*,* κ | susceptibility | 1 → 4π |
| χρ | mass susceptibility | 1 cm3/g → 4π × 10−3 m3/kg |
| μ | permeability | 1 → 4π × 10−7 H/m  = 4π × 10−7 Wb/(A·m) |
| μr | relative permeability | μ → μr |
| *w, W* | energy density | 1 erg/cm3 → 10−1 J/m3 |
| *N, D* | demagnetizing factor | 1 → 1/(4π) |

No vertical lines in table. Statements that serve as captions for the entire table do not need footnote letters.

aGaussian units are the same as cgs emu for magnetostatics; Mx = maxwell, G = gauss, Oe = oersted; Wb = weber, V = volt, s = second, T = tesla, m = meter, A = ampere, J = joule, kg = kilogram, H = henry.

An IEEE copyright form should accompany your final submission. You can get a .pdf, .html, or .doc version at <http://www.ieee.org/copyright> or from the first issues in each volume of the IEEE TRANSACTIONS and JOURNALS*.* Authors are responsible for obtaining any security clearances.

# MATH

If you are using *Word,* use either the Microsoft Equation Editor or the *MathType* add-on (http://www.mathtype.com) for equations in your paper (Insert | Object | Create New | Microsoft Equation *or* MathType Equation). “Float over text” should *not* be selected.

# Units

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). **This applies to papers in data storage.** For example, write “15 Gb/cm2 (100 Gb/in2).” An exception is when English units are used as identifiers in trade, such as “3½ in disk drive.” Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

The SI unit for magnetic field strength *H* is A/m. However, if you wish to use units of T, either refer to magnetic flux density *B* or magnetic field strength symbolized as µ0*H*. Use the center dot to separate compound units, e.g., “A·m2.”

# Helpful Hints

## Figures and Tables

Because IEEE will do the final formatting of your paper, you do not need to position figures and tables at the top and bottom of each column. In fact, all figures, figure captions, and tables can be at the end of the paper. Large figures and tables may span both columns. Place figure captions below the figures; place table titles above the tables. If your figure has two parts, include the labels “(a)” and “(b)” as part of the artwork. Please verify that the figures and tables you mention in the text actually exist. **Please do not include captions as part of the figures. Do not put captions in “text boxes” linked to the figures. Do not put borders around the outside of your figures.** Use the abbreviation “Fig.” even at the beginning of a sentence. Do not abbreviate “Table.” Tables are numbered with Roman numerals.

Color printing of figures is available, but is billed to the authors (approximately $1300, depending on the number of figures and number of pages containing color). Include a note with your final paper indicating that you request color printing. **Do not use color unless it is necessary for the proper interpretation of your figures.** If you want reprints of your color article, the reprint order should be submitted promptly. There is an additional charge of $81 per 100 for color reprints.

Figure axis labels are often a source of confusion. Use words rather than symbols. As an example, write the quantity “Magnetization,” or “Magnetization *M*,” not just “*M*.” Put units in parentheses. Do not label axes only with units. As in Fig. 1, for example, write “Magnetization (A/m)” or “Magnetization (Am−1),” not just “A/m.” Do not label axes with a ratio of quantities and units. For example, write “Temperature (K),” not “Temperature/K.”

Multipliers can be especially confusing. Write “Magnetization (kA/m)” or “Magnetization (103 A/m).” Do not write “Magnetization (A/m) × 1000” because the reader would not know whether the top axis label in Fig. 1 meant 16000 A/m or 0.016 A/m. Figure labels should be legible, approximately 8 to 12 point type.

## References

Number citations consecutively in square brackets [1]. The sentence punctuation follows the brackets [2]. Multiple references [2], [3] are each numbered with separate brackets [1]–[3]. When citing a section in a book, please give the relevant page numbers [2]. In sentences, refer simply to the reference number, as in [3]. Do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] shows ... .” Unfortunately the IEEE document translator cannot handle automatic endnotes in *Word*; therefore, type the reference list at the end of the paper using the “References” style.

Number footnotes separately in superscripts (Insert | Footnote).[[2]](#footnote-2) Place the actual footnote at the bottom of the column in which it is cited; do not put footnotes in the reference list (endnotes). Use letters for table footnotes (see Table I).

Please note that the references at the end of this document are in the preferred referencing style. Give all authors’ names; do not use “*et al*.” unless there are six authors or more. Use a space after authors' initials. Papers that have not been published should be cited as “unpublished” [4]. Papers that have been submitted for publication should be cited as “submitted for publication” [5]. Papers that have been accepted for publication, but not yet specified for an issue should be cited as “to be published” [6]. Please give affiliations and addresses for private communications [7].

Capitalize only the first word in a paper title, except for proper nouns and element symbols. For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [8].

## Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have already been defined in the abstract. Abbreviations such as IEEE, SI, ac, and dc do not have to be defined. Abbreviations that incorporate periods should not have spaces: write “C.N.R.S.,” not “C. N. R. S.” Do not use abbreviations in the title unless they are unavoidable (for example, “IEEE” in the title of this article).

## Equations

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). First use the equation editor to create the equation. Then select the “Equation” markup style. Press the tab key and write the equation number in parentheses. To make your equations more compact, you may use the solidus ( / ), the exp function, or appropriate exponents. Use parentheses to avoid ambiguities in denominators. Punctuate equations when they are part of a sentence, as in

(1)

Be sure that the symbols in your equation have been defined before the equation appears or immediately following. Italicize symbols (*T* might refer to temperature, but T is the unit tesla). Refer to “(1),” not “Eq. (1)” or “equation (1),” except at the beginning of a sentence: “Equation (1) is ... .”

## Other Recommendations

Use one space after periods and colons. Hyphenate complex modifiers: “zero-field-cooled magnetization.” Avoid dangling participles, such as, “Using (1), the potential was calculated.” [It is not clear who or what used (1).] Write instead, “The potential was calculated by using (1),” or “Using (1), we calculated the potential.”

Use a zero before decimal points: “0.25,” not “.25.” Use “cm3,” not “cc.” Indicate sample dimensions as “0.1 cm × 0.2 cm,” not “0.1 × 0.2 cm2.” The abbreviation for “seconds” is “s,” not “sec.” Do not mix complete spellings and abbreviations of units: use “Wb/m2” or “webers per square meter,” not “webers/m2.” When expressing a range of values, write “7 to 9” or “7-9,” not “7~9.”

A parenthetical statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.) In American English, periods and commas are within quotation marks, like “this period.” Other punctuation is “outside”! Avoid contractions; for example, write “do not” instead of “don’t.” The serial comma is preferred: “A, B, and C” instead of “A, B and C.”

If you wish, you may write in the first person singular or plural and use the active voice (“I observed that ...” or “We observed that ...” instead of “It was observed that ...”). Remember to check spelling. If your native language is not English, please get a native English-speaking colleague to proofread your paper.

# Some Common Mistakes

The word “data” is plural, not singular. The subscript for the permeability of vacuum µ0 is zero, not a lowercase letter “o.” The term for residual magnetization is “remanence”; the adjective is “remanent”; do not write “remnance” or “remnant.” Use the word “micrometer” instead of “micron.” A graph within a graph is an “inset,” not an “insert.” The word “alternatively” is preferred to the word “alternately” (unless you really mean something that alternates). Use the word “whereas” instead of “while” (unless you are referring to simultaneous events). Do not use the word “essentially” to mean “approximately” or “effectively.” Do not use the word “issue” as a euphemism for “problem.” When compositions are not specified, separate chemical symbols by en-dashes; for example, “NiMn” indicates the intermetallic compound Ni0.5Mn0.5 whereas “Ni–Mn” indicates an alloy of some composition NixMn1-x.

Be aware of the different meanings of the homophones “affect” (usually a verb) and “effect” (usually a noun), “complement” and “compliment,” “discreet” and “discrete,” “principal” (e.g., “principal investigator”) and “principle” (e.g., “principle of measurement”). Do not confuse “imply” and “infer.”

Prefixes such as “non,” “sub,” “micro,” “multi,” and “"ultra” are not independent words; they should be joined to the words they modify, usually without a hyphen. There is no period after the “et” in the Latin abbreviation “*et al.*” (it is also italicized). The abbreviation “i.e.,” means “that is,” and the abbreviation “e.g.,” means “for example” (these abbreviations are not italicized).

An excellent style manual and source of information for science writers is [9]. A general IEEE style guide, *Information for Authors,* is available at <http://www.ieee.org/organizations/pubs/transactions/information.htm>

# Editorial Policy

Submission of a manuscript is not required for participation in a conference. Do not submit a reworked version of a paper you have submitted or published elsewhere. Do not publish “preliminary” data or results. The submitting author is responsible for obtaining agreement of all coauthors and any consent required from sponsors before submitting a paper. IEEE TRANSACTIONS and JOURNALS strongly discourage courtesy authorship. It is the obligation of the authors to cite relevant prior work.

The Transactions and Journals Department does not publish conference records or proceedings. The TRANSACTIONS does publish papers related to conferences that have been recommended for publication on the basis of peer review. As a matter of convenience and service to the technical community, these topical papers are collected and published in one issue of theTRANSACTIONS.

At least two reviews are required for every paper submitted. For conference-related papers, the decision to accept or reject a paper is made by the conference editors and publications committee; the recommendations of the referees are advisory only. Undecipherable English is a valid reason for rejection. Authors of rejected papers may revise and resubmit them to the TRANSACTIONS as regular papers, whereupon they will be reviewed by two new referees.

# Publication Principles

The contents of IEEE TRANSACTIONS and JOURNALS are peer-reviewed and archival. The TRANSACTIONS publishes scholarly articles of archival value as well as tutorial expositions and critical reviews of classical subjects and topics of current interest.

Authors should consider the following points:

1. Technical papers submitted for publication must advance the state of knowledge and must cite relevant prior work.
2. The length of a submitted paper should be commensurate with the importance, or appropriate to the complexity, of the work. For example, an obvious extension of previously published work might not be appropriate for publication or might be adequately treated in just a few pages.
3. Authors must convince both peer reviewers and the editors of the scientific and technical merit of a paper; the standards of proof are higher when extraordinary or unexpected results are reported.
4. Because replication is required for scientific progress, papers submitted for publication must provide sufficient information to allow readers to perform similar experiments or calculations and use the reported results. Although not everything need be disclosed, a paper must contain new, useable, and fully described information. For example, a specimen's chemical composition need not be reported if the main purpose of a paper is to introduce a new measurement technique. Authors should expect to be challenged by reviewers if the results are not supported by adequate data and critical details.
5. Papers that describe ongoing work or announce the latest technical achievement, which are suitable for presentation at a professional conference, may not be appropriate for publication in a TRANSACTIONS or JOURNAL.

# Conclusion

A conclusion section is not required. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

References

1. G. O. Young, “Synthetic structure of industrial plastics (Book style with paper title and editor),” in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
2. W.-K. Chen, *Linear Networks and Systems* (Book style)*.* Belmont, CA: Wadsworth, 1993, pp. 123–135.
3. H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
4. B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.
5. E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” *IEEE Trans. Antennas Propagat.*, to be published.
6. J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” *IEEE J. Quantum Electron.*, submitted for publication.
7. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
8. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style),” *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].
9. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.
10. J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” *IEEE Trans. Electron Devices*, vol. ED-11, pp. 34–39, Jan. 1959.
11. S. Chen, B. Mulgrew, and P. M. Grant, “A clustering technique for digital communications channel equalization using radial basis function networks,” *IEEE Trans. Neural Networks*, vol. 4, pp. 570–578, July 1993.
12. R. W. Lucky, “Automatic equalization for digital communication,” *Bell Syst. Tech. J.*, vol. 44, no. 4, pp. 547–588, Apr. 1965.
13. S. P. Bingulac, “On the compatibility of adaptive controllers (Published Conference Proceedings style),” in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8–16.
14. G. R. Faulhaber, “Design of service systems with priority reservation,” in *Conf. Rec. 1995 IEEE Int. Conf. Communications,* pp. 3–8.
15. W. D. Doyle, “Magnetization reversal in films with biaxial anisotropy,” in *1987 Proc. INTERMAG Conf.*, pp. 2.2-1–2.2-6.
16. G. W. Juette and L. E. Zeffanella, “Radio noise currents n short sections on bundle conductors (Presented Conference Paper style),” presented at the IEEE Summer power Meeting, Dallas, TX, June 22–27, 1990, Paper 90 SM 690-0 PWRS.
17. J. G. Kreifeldt, “An analysis of surface-detected EMG as an amplitude-modulated noise,” presented at the 1989 Int. Conf. Medicine and Biological Engineering, Chicago, IL.
18. J. Williams, “Narrow-band analyzer (Thesis or Dissertation style),” Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.
19. N. Kawasaki, “Parametric study of thermal and chemical nonequilibrium nozzle flow,” M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.
20. J. P. Wilkinson, “Nonlinear resonant circuit devices (Patent style),” U.S. Patent 3 624 12, July 16, 1990.
21. *IEEE Criteria for Class IE Electric Systems* (Standards style)*,* IEEE Standard 308, 1969.
22. *Letter Symbols for Quantities*, ANSI Standard Y10.5-1968.
23. R. E. Haskell and C. T. Case, “Transient signal propagation in lossless isotropic plasmas (Report style),” USAF Cambridge Res. Lab., Cambridge, MA Rep. ARCRL-66-234 (II), 1994, vol. 2.
24. E. E. Reber, R. L. Michell, and C. J. Carter, “Oxygen absorption in the Earth’s atmosphere,” Aerospace Corp., Los Angeles, CA, Tech. Rep. TR-0200 (420-46)-3, Nov. 1988.
25. (Handbook style) *Transmission Systems for Communications,* 3rd ed., Western Electric Co., Winston-Salem, NC, 1985, pp. 44–60.
26. *Motorola Semiconductor Data Manual,* Motorola Semiconductor Products Inc., Phoenix, AZ, 1989.
27. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume(issue). Available: <http://www.(URL>)
28. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: <http://www.atm.com>
29. (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: <http://www.(URL>)
30. R. J. Vidmar. (1992, August). On the use of atmospheric plasmas as electromagnetic reflectors. *IEEE Trans. Plasma Sci.* [Online]. *21(3).* pp. 876—880. Available: http://www.halcyon.com/pub/journals/21ps03-vidmar

1. Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Depart­ment of Com­merce under Grant BS123456 (sponsor and financial support acknowledgment goes here). [↑](#footnote-ref-1)
2. It is recommended that footnotes be avoided (except for the unnumbered footnote with the receipt date on the first page). Instead, try to integrate the footnote information into the text. [↑](#footnote-ref-2)