Secure Third-party Fast Covariance Intersection using Partially Homomorphic and Order Revealing Encryption Schemes

Marko Ristic, Benjamin Noack, and Uwe D. Hanebeck

***Abstract*— Fast covariance intersection is a widespread technique for state estimate fusion in sensor networks when cross-correlations are not known and fast computations are desired. The common requirement of sending estimates from one party to another during fusion means they do not remain private to their producing party. Current secure fusion algorithms have a reliance on encryption schemes that do not provide sufficient flexibility and as a result require, often undesired, excess communication between estimate producers. We propose a novel method of homomorphically computing the fast covariance intersection algorithm on estimates encrypted with a combination of encryption schemes. Using order revealing encryption we show how to approximate solutions to the fast covariance intersection coefficients can be computed and combined with partially homomorphic encryptions of estimates, to compute an encryption of the fused result. The described approach allows the secure fusion of any number of private estimates, making third-party cloud processing a viable option when working with sensitive state estimates, or when performing estimation over insecure networks.**

I. Introduction

-
- Describe what will be in each following section and how the paper structure makes sense

A. Notation

- Brief overview of ISAS vector and random vector notation
- Encryption notation, keys omitted where it's obvious from context
- Encryption of matrices and vectors is element-wise
- Real number encoding assumed in all encryption notation, all numbers are real

II. Covariance Intersection and Approximations

- Covariance intersection (CI) is a method for fusing state estimations for different sources when models and cross-correlations are not known
- The fused estimate and estimate covariance are commuted by (1) and (2)
- Note that the estimate and estimate covariance depicted in (1) and (2) are in the Information filter form of the popular Kalman Filter as this simplifies computation.

Marko Ristic, Benjamin Noack, and Uwe D. Hanebeck are with the Intelligent Sensor-Actuator-Systems Laboratory (ISAS), Institute for Anthropomatics, Karlsruhe Institute of Technology (KIT), Germany.
{marko.ristic,noack,uwe.hanebeck}@kit.edu

$$\mathbf{P}^{-1} = \sum_{i=0}^{n} \omega_i \mathbf{P}_i^{-1} \tag{1}$$

$$\mathbf{P}^{-1}\underline{\hat{x}} = \sum_{i=0}^{n} \omega_i \mathbf{P}_i^{-1}\underline{\hat{x}}_i \tag{2}$$

$$\tag{3}$$

- Where values ω_i satisfy (4) and (5) and are chosen in a way to minimise a property of the resulting fused estimate.
- For example minimising the resulting trace would require solving (6)

$$\omega_0 + \omega_1 + \cdots + \omega_n = 1 \tag{4}$$

$$0 \leq \omega_i \leq 1 \tag{5}$$

$$\underset{\omega_0,\ldots,\omega_n}{\arg\min}\{\operatorname{tr}(\mathbf{P})\} = \underset{\omega_0,\ldots,\omega_n}{\arg\min}\{\operatorname{tr}((\sum_{i=0}^{n} \omega_i \mathbf{P}_i)^{-1})\} \tag{6}$$

- Minimising a given non linear cost function such as (6) can be very costly computationally and has led to the development of non-iterative approximation techniques [1], [2], [3]

A. Fast Covariance intersection

- The fast covariance intersection (FCI) algorithm described in [1] is a common method used for approximating the solution to (6) by defining a new constraint on ω_i and solving that instead.
- In the 2 sensor case, (4) now becomes (7), and the additional requirement of (8) is also defined. Solutions are defined analytically and shown in (9)

$$\omega_0 + \omega_1 = 1 \tag{7}$$

$$\omega_0 \operatorname{tr}(\mathbf{P}_0) - \omega_1 \operatorname{tr}(\mathbf{P}_1) = 0 \tag{8}$$

$$\omega_0 = \frac{\operatorname{tr}(\mathbf{P}_1)}{\operatorname{tr}(\mathbf{P}_0) + \operatorname{tr}(\mathbf{P}_1)},\ \omega_1 = \frac{\operatorname{tr}(\mathbf{P}_0)}{\operatorname{tr}(\mathbf{P}_0) + \operatorname{tr}(\mathbf{P}_1)} \tag{9}$$

- When extending to any number of sensors, restriction (8) is generalised to (10)

$$\omega_i \operatorname{tr}(\mathbf{P}_i) - \omega_j \operatorname{tr}(\mathbf{P}_j) = 0,\ (i,j = 1,2,\ldots,n) \tag{10}$$

- Equation (10) is highly redundant and its largest linearly independent subset can be represented with (11).

$$\omega_i \operatorname{tr}(\mathbf{P}_i) - \omega_{i+1} \operatorname{tr}(\mathbf{P}_{i+1}) = 0,\ (i = 1,2,\ldots,n) \tag{11}$$

- The solution to (11) and (4) can be represented as the simultaneous equations problem shown in (12) where $\mathcal{P}_i = \operatorname{tr}(\mathbf{P}_i)$

$$\begin{bmatrix} \mathcal{P}_0 & -\mathcal{P}_1 & 0 & \cdots & 0 \\ 0 & \mathcal{P}_1 & -\mathcal{P}_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \mathcal{P}_{n-1} & -\mathcal{P}_n \\ 1 & \cdots & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \omega_0 \\ \omega_0 \\ \vdots \\ \omega_{n-1} \\ \omega_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \tag{12}$$

- Our goal for secure fusion is to solve (1), (2) and (12) using only encryptions from each sensor i.

III. Homomorphic and Order Revealing Encryption

- To achieve a secure solution to the FCI fusion problem, we have focused on two types of function providing encryption schemes.
- Additive partially homomorphic encryption (PHE) schemes such ones defined in [4] and [5] provide a homomorphic addition operation as shown in (13).
- Order revealing encryption (ORE) schemes such as those in [6] and [7] provide a function which allows the comparison of encrypted values as shown in (14)

$$\mathcal{E}(a) \oplus \mathcal{E}(b) = \mathcal{E}(a+b) \tag{13}$$

$$f(\mathcal{E}(a), \mathcal{E}(b)) = cmp(a, b) \tag{14}$$

A. Additive Partially Homomorphic Encryption

- We have used the Paillier encryption scheme described in [4] for the computation of the FCI due to its speed and implementation simplicity.
- The Paillier encryption scheme is a public key scheme, where encryptions are made with a public key but only the secret key holder can decrypt them.
- It provides two homomorphic operations on encrypted data, shown in (15) and (16). The modulus N is computed as a product of 2 large primes which are part of the secret key.

$$\mathcal{E}(a)\mathcal{E}(b) \pmod N = \mathcal{E}(a+b \pmod N) \tag{15}$$

$$\mathcal{E}(a)^c \pmod N = \mathcal{E}(ca \pmod N),\ c \in \mathbb{Z}_N \tag{16}$$

- Encrypted numbers must be less than N, and negative numbers can be handled by storing integers in "two's complement" binary form, that is taking $[0, \frac{N}{2})$ as all possible positive numbers, and $[\frac{N}{2}, N)$ as the decreasing negative integers.

B. Real Number Encoding for Homomorphic Encryption

- The Paillier encryption scheme can only encrypt, add, and multiply with integers. Due to the prevalence of real number values in sensor outputs and estimation processes, some form of encoding is required for these numbers to be encrypted.
- Real numbers, typically stored as floating-point numbers in sensor hardware, are converted to integers using the "Q" number format. A real number a can be encoded to an integer e using (17), where the largest encodable real number has an integer part of i bits. Integer bits i and fractional bits f are chosen such that the largest encoded value can still be encrypted.

$$e = \begin{cases} \lfloor 2^f a \rfloor & a < 2^i \\ \lfloor 2^f (2^i - a) \rfloor & a \geq 2^i \end{cases} \tag{17}$$

- While the encoded real numbers are consistent under addition, multiplication by constants requires that a factor of $\frac{1}{2^f}$ be removed.
- Since division is not supported under the encryption scheme, the number of multiplications performed on an encrypted value must be bounded and handled when decoding. This also decreases the size of the largest encodable real number that can be decoded correctly.
- In our case, only a single multiplication is required, and decoding of an integer e to a real number f is performed by (18).

$$a = \begin{cases} \frac{e}{2^f} & e < 2^{(i+f)} \\ \frac{e}{2^{2f}} & e \geq 2^{(i+f)} \end{cases} \tag{18}$$

C. Left-Right Order Revealing Encryption

- For the ORE scheme we have considered in particular the Left-Right encryption scheme described in [7] which will help in preventing information leakage as described in section IV.
- The key difference between this scheme and others is how numbers are compared. Left-Right encryption allows any number to be encrypted as either a "Left" or "Right" encryption, but only a "Left" encryption can be compared with a "Right" encryption. The provided function of the encryption scheme are shown in (19)
- The ORE scheme described requires a single symmetric key for the encryption of either "Left" or "Right" encryptions, which can be compared without any key.

$$encrypt^L_{ORE}(sk, x) = \mathcal{E}^L_{ORE}(x) \tag{19}$$

$$encrypt^R_{ORE}(sk, y) = \mathcal{E}^R_{ORE}(y) \tag{20}$$

$$compare_{ORE}(\mathcal{E}^L_{ORE}(x),\ \mathcal{E}^R_{ORE}(y)) = cmp(x, y) \tag{21}$$

IV. Secure Fast Covariance Intersection with 2 Sensors

- First we will consider the 2 sensor case of secure FCI (SecFCI), before extending it to any number of sensors in section V. We consider sensor 0 which produces the estimate $\underline{\hat{x}}_0$ and covariance $\mathbf{P}_0$, and similarly sensor 1 producing $\underline{\hat{x}}_1$ and $\mathbf{P}_1$.
- From (1) and (2) we can see that CI is particularly suited to PHE schemes. Sensor encrypted estimates and covariances can be combined additively using (15) and (16). The equations using the Paillier encrtyption systems to compute CI are given in (22) and (23).

$$\mathcal{E}(\mathbf{P}) = \mathcal{E}(\mathbf{P}_0)^{\omega_0} \mathcal{E}(\mathbf{P}_1)^{(1-\omega_0)} \tag{22}$$

$$\mathcal{E}(\mathbf{P}\underline{\hat{x}}) = \mathcal{E}(\mathbf{P}_0\underline{\hat{x}}_0)^{\omega_0} \mathcal{E}(\mathbf{P}_1\underline{\hat{x}}_1)^{(1-\omega_0)} \tag{23}$$

$$\tag{24}$$

- What remains is the computation of the parameter ω. The FCI solutions for the 2 sensor case given by (9), cannot be computed with PHE encryptions due to the required division.
- Instead we discretise ω to steps of some size $s < 1$ such that s divides 1, and use the ORE scheme to compute (8). Each sensor discretises ω and multiplies each discretisation with $\mathrm{tr}(\mathbf{P}^{-1})$ of its current coveriance $\mathbf{P}$. Each result is then encrypted with the Left-Right ORE scheme.
- Sensor 0 encrypts using the Left scheme as shown in (25) and similarly for sensor 1 using Right encryption in (26).

$$[\mathcal{E}^L_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_0^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]] \tag{25}$$
$$[\mathcal{E}^R_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_1^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]] \tag{26}$$

- The two ordered encrypted lists (25) and (26) are recieved at the fusion center, and used to estimate ω.
- To compute the FCI value for ω we want the intersection between the two lines described by $\mathrm{tr}(\mathbf{P}_0)\omega$ and $\mathrm{tr}(\mathbf{P}_1)(1-\omega)$. Note that in the 2 sensor case, the discretised list of $\mathrm{tr}(\mathbf{P}_i)(1-\omega)$ can be obtained by simply reversing the list for $\mathrm{tr}(\mathbf{P}_i)\omega$.
- Fig. 1 shows the list from sensor 0 and the reversed list of sensor 1 plotted over ω with a step size $s = 0.1$. Since values from one list can be compared with those from the other using the ORE operations described in (19), the exact intersection can be approximated in $O(log(\frac{1}{s}))$ steps by performing a binary search.

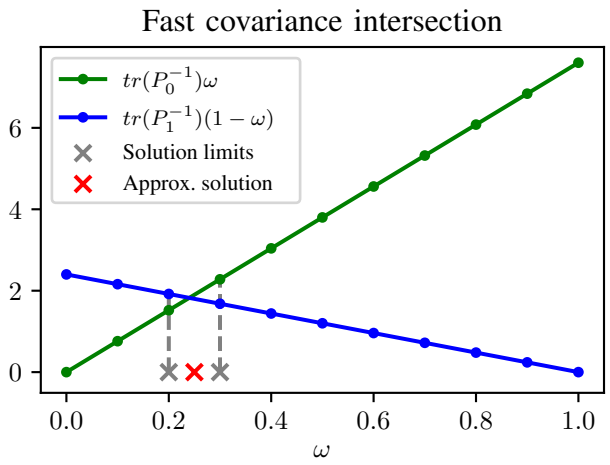

Fig. 1. Approximation of ω_0 with discretisation step size $s = 0.1$. Only comparisons of the ordered values sent from either estimator are used.

- Once the two consecutive differing comparisons from vertically aligned points in 1 are found, the FCI ω can be approximated by taking the middle value between the two bounds. This is computed simply with (27).
- In the case where the comparison function from the ORE scheme returns an exact equality, the exact value of ω is known and can be taken as the approximation.

$$\omega_0' = \frac{1}{2}(a+b),\ \omega_1' = (1-\omega_0) \tag{27}$$

V. Multi-sensor Secure Fast Covariance Intersection

-

$$\omega_0\,\mathrm{tr}(\mathbf{P}_0) - \omega_1\,\mathrm{tr}(\mathbf{P}_1) = 0 \tag{28}$$

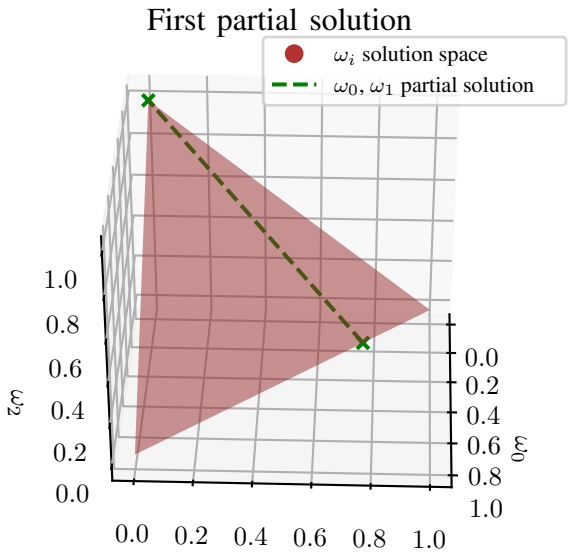

Fig. 2. Partial solution from equation (28) plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

$$\omega_1\,\mathrm{tr}(\mathbf{P}_1) - \omega_2\,\mathrm{tr}(\mathbf{P}_2) = 0 \tag{29}$$

$$a_0x + a_1y + a_2z + d = 0 \tag{30}$$

$$\begin{bmatrix} a_0^0 & a_0^1 & a_0^2 \\ a_0^1 & a_1^1 & a_2^1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \omega_0 \\ \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} d^0 \\ d^1 \\ 1 \end{bmatrix} \tag{31}$$

$$\begin{bmatrix} a_0^0 & a_1^0 & \cdots & a_n^0 \\ a_0^1 & a_1^1 & \cdots & a_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^n & a_1^n & \cdots & a_n^{n-1} \\ 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \omega_0 \\ \omega_1 \\ \vdots \\ \omega_{n-1} \\ \omega_n \end{bmatrix} = \begin{bmatrix} d^0 \\ d^1 \\ \vdots \\ d^{n-1} \\ 1 \end{bmatrix} \tag{32}$$

$$[\mathcal{E}^L_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is even} \tag{33}$$

$$[\mathcal{E}^R_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is odd} \tag{34}$$

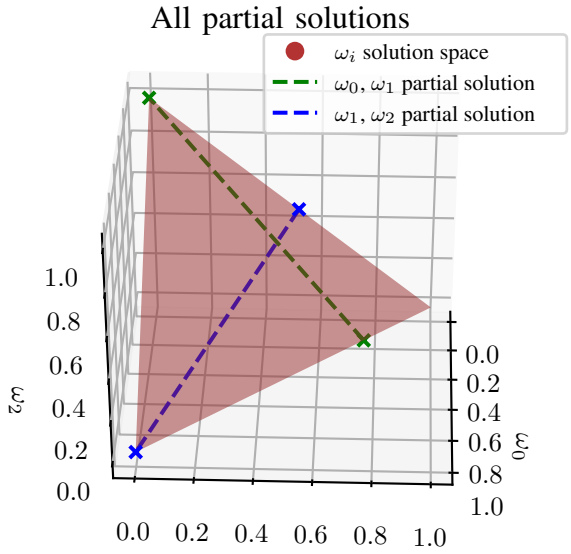

Fig. 3. Partial solutions from equations (28) and (29) plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

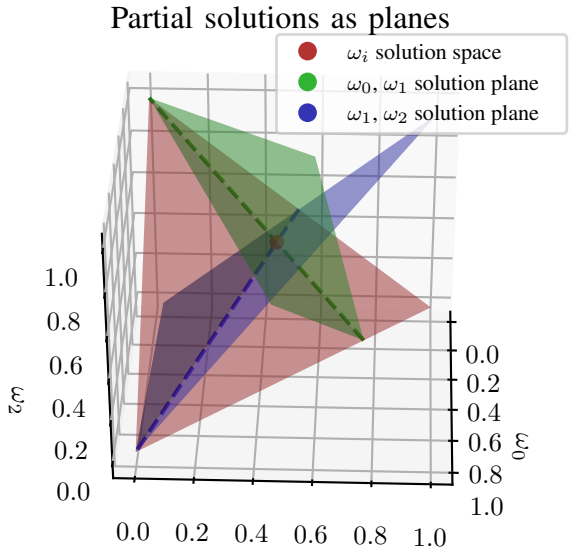

Fig. 4. Partial solutions from fig. 3 plotted as planes perpendicular to the plane of possible solutions. Intersection point gives solution values of ω_i for Fast Covariance Intersection.

VI. Simulation Results

VII. Conclusion

VIII. Introduction

This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. All standard paper components have been specified for three reasons: (1) ease of use when formatting individual papers, (2) automatic compliance to electronic requirements that facilitate the concurrent or later production of electronic products, and (3) conformity of style throughout a conference proceedings. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

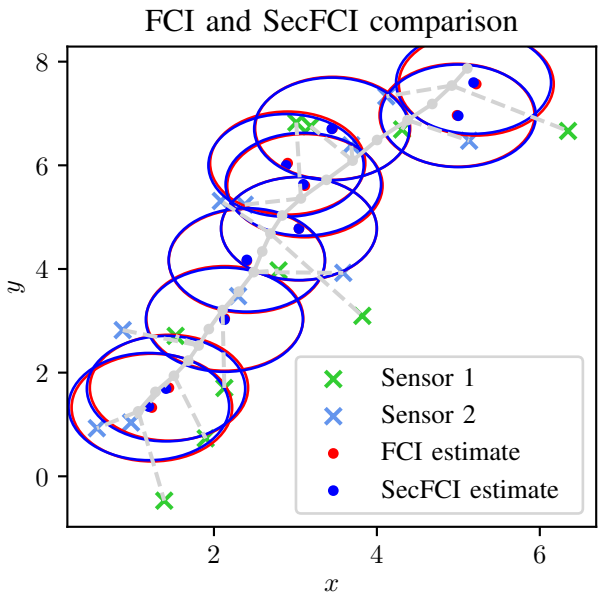

Fig. 5. Tracking simulation comparing Fast Covariance Intersection and our Secure Fast Covariance Intersection fusion methods.

IX. Procedure for Paper Submission

A. Selecting a Template (Heading 2)

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. It may be used for A4 paper size if the paper size setting is suitably modified.

B. Maintaining the Integrity of the Specifications

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations

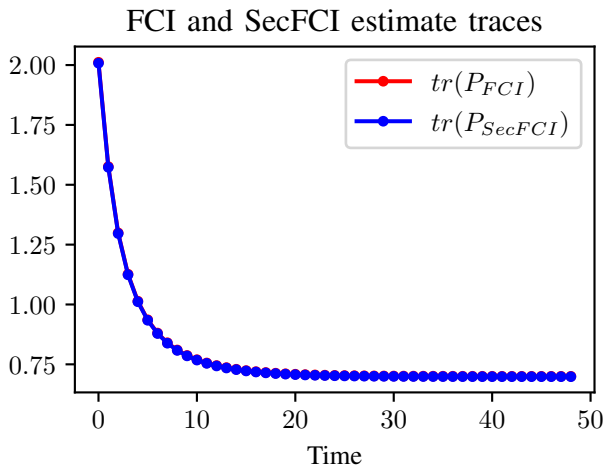

Fig. 6. Plot showing the fused estimate covariance trace throughout a tracking simulation, for both Fast Covariance Intersection and our Secure Fast Covariance Intersection

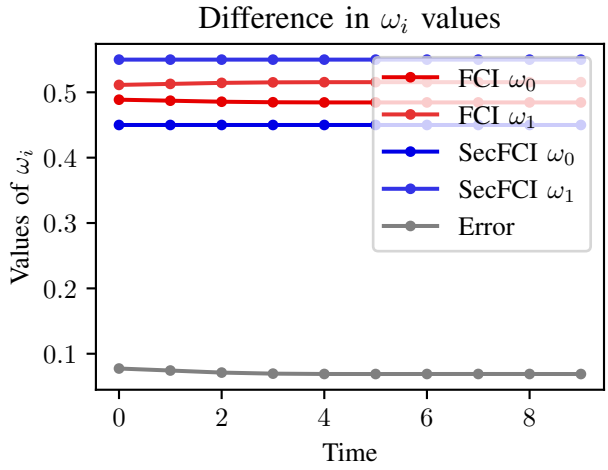

Fig. 7. Plot showing the difference in ω_i values between Fast Covariance Intersection and our Secure Fast Covariance Intersection, throughout a tracking simulation.

X. MATH

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

A. Abbreviations and Acronyms

Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable.

B. Units

- Use either SI (MKS) or CGS as primary units. (SI units are encouraged.) English units may be used as secondary units (in parentheses). An exception would be the use of English units as identifiers in trade, such as Ò3.5-inch disk driveÓ.
- 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 that you use in an equation.
- Do not mix complete spellings and abbreviations of units: ÒWb/m2Ó or Òwebers per square meterÓ, not Òwebers/m2Ó. Spell out units when they appear in text: Ò. . . a few henriesÓ, not Ò. . . a few HÓ.
- Use a zero before decimal points: Ò0.25Ó, not Ò.25Ó. Use Òcm3Ó, not ÒccÓ. (bullet list)

C. Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled. Number equations consecutively. Equation numbers, within parentheses, are to position flush right, as in (1), using a right tab stop. To make your equations more compact, you may use the solidus (/), the exp function, or appropriate exponents. Italicize Roman symbols for quantities and variables, but not Greek symbols. Use a long dash rather than a hyphen for a minus sign. Punctuate equations with commas or periods when they are part of a sentence, as in

$$\alpha + \beta = \chi \tag{1}$$

Note that the equation is centered using a center tab stop. Be sure that the symbols in your equation have been defined before or immediately following the equation. Use Ò(1)Ó, not ÒEq. (1)Ó or Òequation (1)Ó, except at the beginning of a sentence: ÒEquation (1) is . . .Ó

D. Some Common Mistakes

- The word ÒdataÓ is plural, not singular.
- The subscript for the permeability of vacuum ?0, and other common scientific constants, is zero with subscript formatting, not a lowercase letter ÒoÓ.
- In American English, commas, semi-/colons, periods, question and exclamation marks are located within

quotation marks only when a complete thought or name is cited, such as a title or full quotation. When quotation marks are used, instead of a bold or italic typeface, to highlight a word or phrase, punctuation should appear outside of the quotation marks. A parenthetical phrase or statement at the end of a sentence is punctuated outside of the closing parenthesis (like this). (A parenthetical sentence is punctuated within the parentheses.)

- A graph within a graph is an ÒinsetÓ, not an ÒinsertÓ. The word alternatively is preferred to the word ÒalternatelyÓ (unless you really mean something that alternates).
- Do not use the word ÒessentiallyÓ to mean ÒapproximatelyÓ or ÒeffectivelyÓ.
- In your paper title, if the words Òthat usesÓ can accurately replace the word ÒusingÓ, capitalize the ÒuÓ; if not, keep using lower-cased.
- Be aware of the different meanings of the homophones ÒaffectÓ and ÒeffectÓ, ÒcomplementÓ and ÒcomplimentÓ, ÒdiscreetÓ and ÒdiscreteÓ, ÒprincipalÓ and ÒprincipleÓ.
- Do not confuse ÒimplyÓ and ÒinferÓ.
- The prefix ÒnonÓ is not a word; it should be joined to the word it modifies, usually without a hyphen.
- There is no period after the ÒetÓ in the Latin abbreviation Òet al.Ó.
- The abbreviation Òi.e.Ó means Òthat isÓ, and the abbreviation Òe.g.Ó means Òfor exampleÓ.

XI. USING THE TEMPLATE

Use this sample document as your LaTeX source file to create your document. Save this file as **root.tex**. You have to make sure to use the cls file that came with this distribution. If you use a different style file, you cannot expect to get required margins. Note also that when you are creating your out PDF file, the source file is only part of the equation. *Your TEX → PDF filter determines the output file size. Even if you make all the specifications to output a letter file in the source - if your filter is set to produce A4, you will only get A4 output.*

It is impossible to account for all possible situation, one would encounter using TEX. If you are using multiple TEX files you must make sure that the "MAIN" source file is called root.tex - this is particularly important if your conference is using PaperPlaza's built in TEX to PDF conversion tool.

A. Headings, etc

Text heads organize the topics on a relational, hierarchical basis. For example, the paper title is the primary text head because all subsequent material relates and elaborates on this one topic. If there are two or more sub-topics, the next level head (uppercase Roman numerals) should be used and, conversely, if there are not at least two sub-topics, then no subheads should be introduced. Styles named ÒHeading 1Ó, ÒHeading 2Ó, ÒHeading 3Ó, and ÒHeading 4Ó are prescribed.

B. Figures and Tables

Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation ÒFig. 1Ó, even at the beginning of a sentence.

TABLE I
AN EXAMPLE OF A TABLE

One	Two
Three	Four

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an document, this method is somewhat more stable than directly inserting a picture.

Fig. 8. Inductance of oscillation winding on amorphous magnetic core versus DC bias magnetic field

Figure Labels: Use 8 point Times New Roman for Figure labels. Use words rather than symbols or abbreviations when writing Figure axis labels to avoid confusing the reader. As an example, write the quantity ÒMagnetizationÓ, or ÒMagnetization, MÓ, not just ÒMÓ. If including units in the label, present them within parentheses. Do not label axes only with units. In the example, write ÒMagnetization (A/m)Ó or ÒMagnetization A[m(1)]Ó, not just ÒA/mÓ. Do not label axes with a ratio of quantities and units. For example, write ÒTemperature (K)Ó, not ÒTemperature/K.Ó

XII. CONCLUSIONS

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.

APPENDIX

Appendixes should appear before the acknowledgment.

ACKNOWLEDGMENT

The preferred spelling of the word ÒacknowledgmentÓ in America is without an ÒeÓ after the ÒgÓ. Avoid the stilted expression, ÒOne of us (R. B. G.) thanks . . .Ó Instead, try ÒR. B. G. thanksÓ. Put sponsor acknowledgments in the unnumbered footnote on the first page.

References are important to the reader; therefore, each citation must be complete and correct. If at all possible, references should be commonly available publications.

REFERENCES

[1] W. Niehsen, "Information fusion based on fast covariance intersection filtering," in *Proceedings of the Fifth International Conference on Information Fusion. FUSION 2002. (IEEE Cat.No.02EX5997)*, vol. 2, Jul. 2002, pp. 901–904 vol.2.

[2] D. Franken and A. Hupper, "Improved fast covariance intersection for distributed data fusion," in *2005 7th International Conference on Information Fusion*, vol. 1, Jul. 2005, pp. 7 pp.–.

[3] J. Cong, Y. Li, G. Qi, and A. Sheng, "An order insensitive sequential fast covariance intersection fusion algorithm," *Information Sciences*, vol. 367-368, pp. 28–40, Nov. 2016.

[4] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," in *Advances in Cryptology — EUROCRYPT '99*, ser. Lecture Notes in Computer Science, J. Stern, Ed. Springer Berlin Heidelberg, 1999, pp. 223–238.

[5] S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[6] N. Chenette, K. Lewi, S. A. Weis, and D. J. Wu, "Practical Order-Revealing Encryption with Limited Leakage," in *Fast Software Encryption*, T. Peyrin, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, vol. 9783, pp. 474–493.

[7] K. Lewi and D. J. Wu, "Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*. Vienna, Austria: ACM Press, 2016, pp. 1167–1178.