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 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

A. Notation

II. Covariance Intersection and Approximations

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

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

$$\omega_0 + \omega_1 + \cdots + \omega_n = 1 \tag{3}$$

$$0 \leq \omega_i \leq 1 \tag{4}$$

$$\underset{\omega_0,\ldots,\omega_n}{\arg\min}\{\operatorname{tr}(\mathbf{P})\} = \underset{\omega_0,\ldots,\omega_n}{\arg\min}\{\operatorname{tr}((\sum_{i=0}^{n} \omega_i \mathbf{P}_i)^{-1})\} \tag{5}$$

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

A. Fast Covariance intersection

$$\omega_0 + \omega_1 = 1 \tag{6}$$

$$\omega_0 \operatorname{tr}(\mathbf{P}_0) - \omega_1 \operatorname{tr}(\mathbf{P}_1) = 0 \tag{7}$$

$$\omega_0 = \frac{\operatorname{tr}(\mathbf{P}_1)}{\operatorname{tr}(\mathbf{P}_0) + \operatorname{tr}(\mathbf{P}_1)},\ \omega_1 = \frac{\operatorname{tr}(\mathbf{P}_0)}{\operatorname{tr}(\mathbf{P}_0) + \operatorname{tr}(\mathbf{P}_1)} \tag{8}$$

$$\omega_i \operatorname{tr}(\mathbf{P}_i) - \omega_j \operatorname{tr}(\mathbf{P}_j) = 0,\ (i,j = 1,2,\ldots,n) \tag{9}$$

$$\omega_i \operatorname{tr}(\mathbf{P}_i) - \omega_{i+1} \operatorname{tr}(\mathbf{P}_{i+1}) = 0,\ (i = 1,2,\ldots,n) \tag{10}$$

$$\mathcal{P}_i = \operatorname{tr}(\mathbf{P}_i) \tag{11}$$

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

III. Homomorphic and Order Revealing Encryption

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

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

A. Additive Partially Homomorphic Encryption

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

$$c \in \mathbb{Z}_N \tag{16}$$

$$\mathcal{E}(a)^c \pmod N = \mathcal{E}(ca \pmod N) \tag{17}$$

B. Real Number Encoding for Homomorphic Encryption

$$e = \lfloor 2^b a \rfloor \tag{18}$$

C. Left-Right Order Revealing Encryption

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

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

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

IV. Secure Fast Covariance Intersection with 2 Sensors

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

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

$$[\mathcal{E}^L_{ORE}(\omega \operatorname{tr}(\mathbf{P}_0^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]] \tag{24}$$

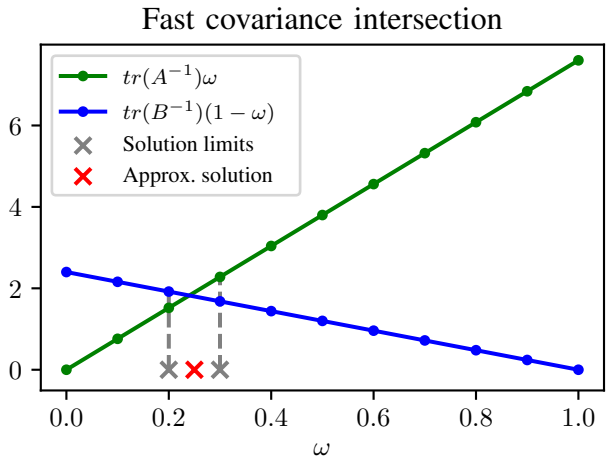

Fig. 1. Approximation of ω_0 with discretisation step size $s = 0.1$. Only comparisons of the ordered values sent from either estimator are used.

$$\omega_0' = \frac{1}{2}(a+b),\ \omega_1' = (1-\omega_0) \tag{25}$$

V. Multi-sensor Secure Fast Covariance Intersection

$$\omega_0 \operatorname{tr}(\mathbf{P}_0) - \omega_1 \operatorname{tr}(\mathbf{P}_1) = 0 \tag{26}$$

$$\omega_1 \operatorname{tr}(\mathbf{P}_1) - \omega_2 \operatorname{tr}(\mathbf{P}_2) = 0 \tag{27}$$

$$a_0 x + a_1 y + a_2 z + d = 0 \tag{28}$$

$$\begin{bmatrix} a_0^0 & a_1^0 & a_2^0 \\ a_0^1 & a_1^1 & a_2^1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \omega_0 \\ \omega_1 \\ \omega_2 \end{bmatrix} = \begin{bmatrix} d^0 \\ d^1 \\ 1 \end{bmatrix} \tag{29}$$

$$\begin{bmatrix} a_0^0 & a_1^0 & \cdots & a_n^0 \\ a_0^1 & a_1^1 & \cdots & a_n^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^n & a_1^n & \cdots & a_n^{n-1} \\ 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} \omega_0 \\ \omega_1 \\ \vdots \\ \omega_{n-1} \\ \omega_n \end{bmatrix} = \begin{bmatrix} d^0 \\ d^1 \\ \vdots \\ d^{n-1} \\ 1 \end{bmatrix} \tag{30}$$

$$[\mathcal{E}^L_{ORE}(\omega \operatorname{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is even} \tag{31}$$

$$[\mathcal{E}^R_{ORE}(\omega \operatorname{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is odd} \tag{32}$$

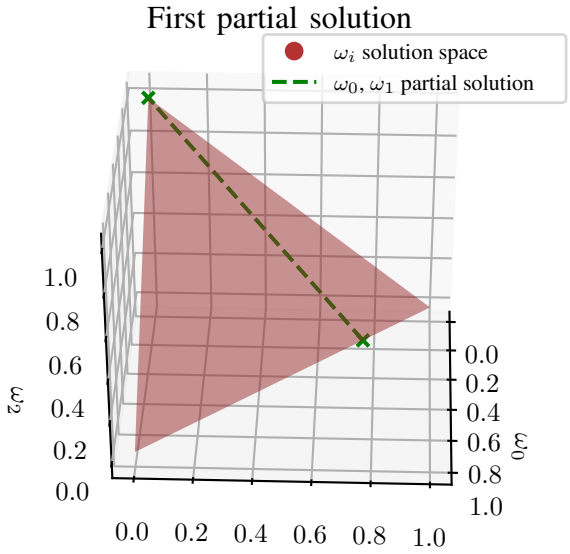

Fig. 2. Partial solution from equation 26 plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

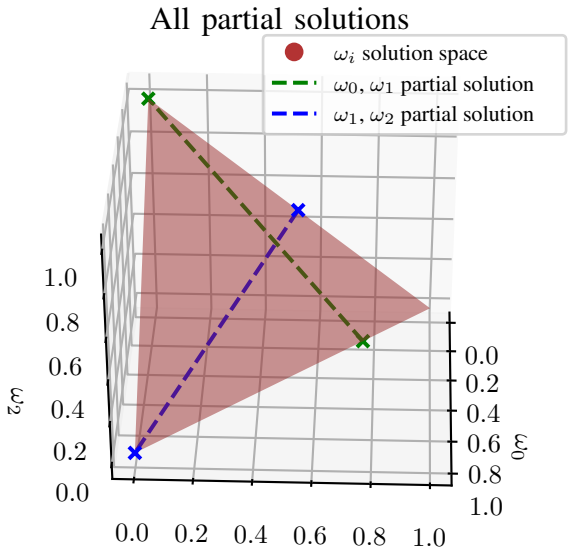

Fig. 3. Partial solutions from equations 26 and 27 plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

VI. Simulation Results

VII. Conclusion

VIII. INTRODUCTION

Your goal is to simulate, as closely as possible, the usual appearance of typeset papers. This document provides an example of the desired layout and contains information

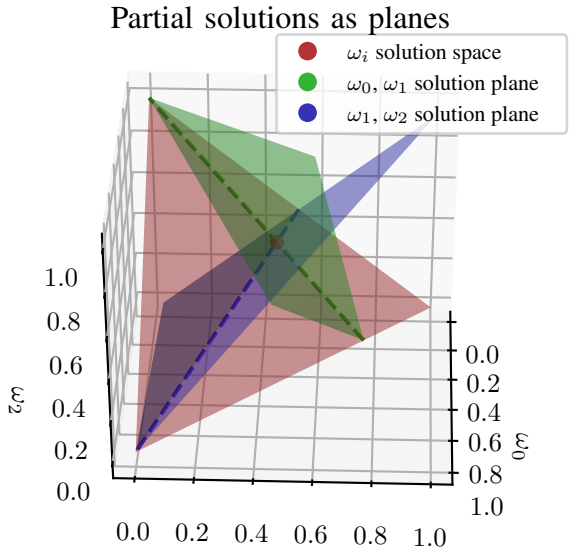

Fig. 4. Partial solutions from figure 3 plotted as planes perpendicular to the plane of possible solutions. Intersection point gives solution values of ω_i for Fast Covariance Intersection.

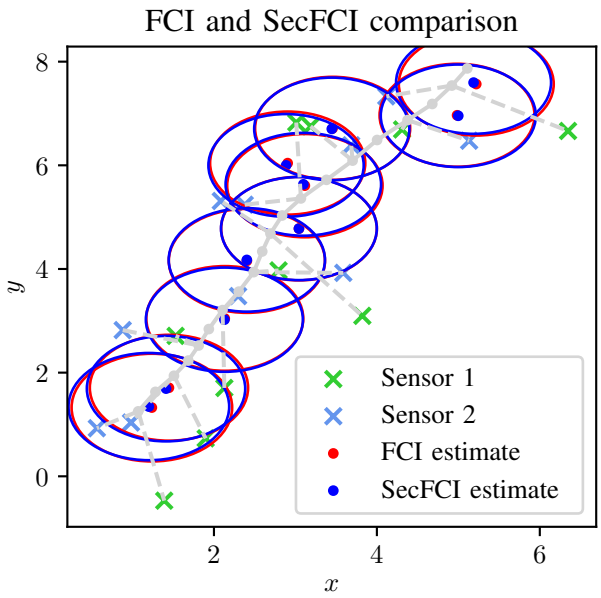

Fig. 5. Tracking simulation comparing Fast Covariance Intersection and our Secure Fast Covariance Intersection fusion methods.

regarding desktop publishing format, type sizes, and type faces.

A. Full-Size Camera-Ready (CR) Copy

If you have desktop publishing facilities, (the use of a computer to aid in the assembly of words and illustrations on pages) prepare your CR paper in full-size format, on paper 21.6 x 27.9 cm (8.5 x 11 in or 51 x 66 picas). It must be output on a printer (e.g., laser printer) having 300 dots/in, or better, resolution. Lesser quality printers, such as dot matrix printers, are not acceptable, as the manuscript will not reproduce the desired quality.

1) Typefaces and Sizes:: There are many different typefaces and a large variety of fonts (a complete set of characters in the same typeface, style, and size). Please use a proportional serif typeface such as Times Roman, or Dutch. If these are not available to you, use the closest typeface you can. The minimum typesize for the body of the text is 10 point. The minimum size for applications like table captions, footnotes, and text subscripts is 8 point. As an aid in gauging type size, 1 point is about 0.35 mm (1/72in). Examples are as follows:

2) Format:: In formatting your original 8.5" x 11" page, set top and bottom margins to 25 mm (1 in or 6 picas), and left and right margins to about 18 mm (0.7 in or 4 picas). The column width is 88 mm (3.5 in or 21 picas). The space between the two columns is 5 mm(0.2 in or 1 pica). Paragraph indentation is about 3.5 mm (0.14 in or 1 pica). Left- and right-justify your columns. Cut A4 papers to 28 cm. Use either one or two spaces between sections, and between text and tables or figures, to adjust the column length. On the last page of your paper, try to adjust the lengths of the two-columns so that they are the same. Use

TABLE I
AN EXAMPLE OF A TABLE

One	Two
Three	Four

automatic hyphenation and check spelling. Either digitize or paste your figures.

IX. UNITS

Metric units are preferred for use in IEEE publications in light of their international readership and the inherent convenience of these units in many fields. In particular, the use of the International System of Units (SI Units) is advocated. This system includes a subsystem the MKSA units, which are based on the meter, kilogram, second, and ampere. British units may be used as secondary units (in parenthesis). An exception is when British units are used as identifiers in trade, such as, 3.5 inch disk drive.

X. ADDITIONAL REQUIREMENTS

A. Figures and Tables

Position figures and tables at the tops and bottoms 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 captions should be above the tables. Avoid placing figures and tables before their first mention in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence. Figure axis labels are often a source of confusion. Try to use words rather then symbols. As an example write the quantity "Inductance", or "Inductance L", not just. Put units in parentheses.

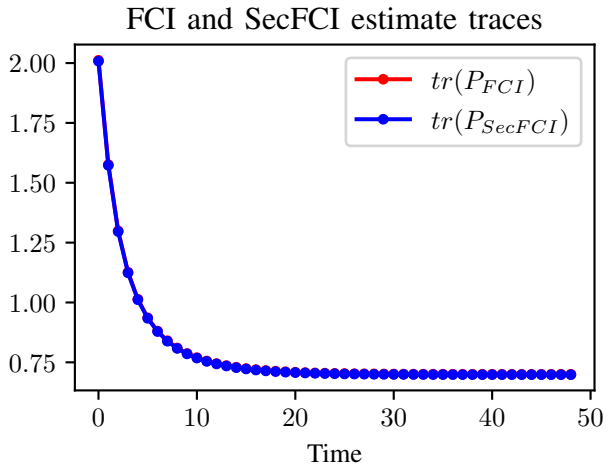

Fig. 6. Plot showing the fused estimate covariance trace over the course of a tracking simulation, for both Fast Covariance Intersection and our Secure Fast Covariance Intersection

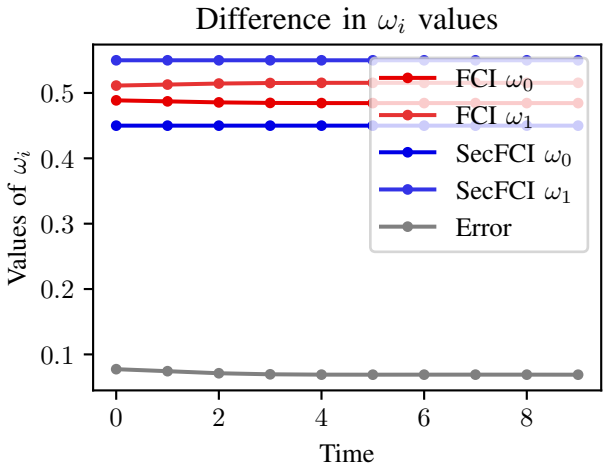

Fig. 7. Plot showing the difference in ω_i values between Fast Covariance Intersection and our Secure Fast Covariance Intersection, over the course of a tracking simulation.

Do not label axes only with units. In the example, write "Inductance (mH)", or "Inductance L (mH)", not just "mH". Do not label axes with the ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

B. Numbering

Number footnotes separately in superscripts[1] Place the actual footnote at the bottom of the column in which it is cited. Do not put footnotes in the reference list. Use letters for table footnotes (see Table I).

C. 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, CGS, ac, dc, and rms do not have to be defined. Do not use abbreviations in the title unless they are unavoidable.

D. Equations

Number equations consecutively with equation numbers in parentheses flush with the right margin, as in (1). 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 then hyphen for a minus sign. Use parentheses to avoid ambiguities in the denominator.

[1]This is a footnote

Punctuate equations with commas or periods when they are part of a sentence:

$$\Gamma_2 a^2 + \Gamma_3 a^3 + \Gamma_4 a^4 + ... = \lambda\Lambda(x),$$

where λ is an auxiliary parameter.

Be sure that the symbols in your equation have been defined before the equation appears or immediately following. Use "(1)," not "Eq. (1)" or "Equation (1)," except at the beginning of a sentence: "Equation (1) is ...".

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

XI. CONCLUSIONS AND FUTURE WORKS

A. Conclusions

This is a repeat. Position figures and tables at the tops and bottoms 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 captions should be above the tables. Avoid placing figures and tables before their first mention in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence. Figure axis labels are often a source of confusion. Try to use words rather then symbols. As an example write the quantity "Inductance", or "Inductance L", not just. Put units in parentheses. Do not label axes only with units. In the example, write "Inductance (mH)", or "Inductance L

(mH)", not just "mH". Do not label axes with the ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

B. Future Works

This is a repeat. Position figures and tables at the tops and bottoms 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 captions should be above the tables. Avoid placing figures and tables before their first mention in the text. Use the abbreviation "Fig. 1", even at the beginning of a sentence. Figure axis labels are often a source of confusion. Try to use words rather then symbols. As an example write the quantity "Inductance", or "Inductance L", not just. Put units in parentheses. Do not label axes only with units. In the example, write "Inductance (mH)", or "Inductance L (mH)", not just "mH". Do not label axes with the ratio of quantities and units. For example, write "Temperature (K)", not "Temperature/K".

XII. ACKNOWLEDGMENTS

The authors gratefully acknowledge the contribution of National Research Organization and reviewers' comments.

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] J.G.F. Francis, The QR Transformation I, *Comput. J.*, vol. 4, 1961, pp 265-271.

[2] H. Kwakernaak and R. Sivan, *Modern Signals and Systems*, Prentice Hall, Englewood Cliffs, NJ; 1991.

[3] D. Boley and R. Maier, "A Parallel QR Algorithm for the Non-Symmetric Eigenvalue Algorithm", *in Third SIAM Conference on Applied Linear Algebra*, Madison, WI, 1988, pp. A20.