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.

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

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

$$\tag{3}$$

- 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)

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

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

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

- 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)

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

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

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

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

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

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

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

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

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

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

- 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.

$$\begin{aligned} encrypt^L_{ORE}(sk, x) &= \mathcal{E}^L_{ORE}(x) \\ encrypt^R_{ORE}(sk, y) &= \mathcal{E}^R_{ORE}(y) \\ compare_{ORE}(\mathcal{E}^L_{ORE}(x),\ \mathcal{E}^R_{ORE}(y)) &= cmp(x,y) \end{aligned} \tag{19}$$

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 (20) and (21).

$$\mathcal{E}(\mathbf{P}) = \mathcal{E}(\mathbf{P}_0)^{\omega_0}\mathcal{E}(\mathbf{P}_1)^{(1-\omega_0)} \tag{20}$$

$$\mathcal{E}(\mathbf{P}\underline{\hat{x}}) = \mathcal{E}(\mathbf{P}_0\underline{\hat{x}}_0)^{\omega_0}\mathcal{E}(\mathbf{P}_1\underline{\hat{x}}_1)^{(1-\omega_0)} \tag{21}$$

$$\tag{22}$$

- 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 (23) and similarly for sensor 1 using Right encryption in (24).

$$[\mathcal{E}^{L}_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_0^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]] \tag{23}$$
$$[\mathcal{E}^{R}_{ORE}(\omega\,\mathrm{tr}(\mathbf{P}_1^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]] \tag{24}$$

- The two ordered encrypted lists (23) and (24) 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.

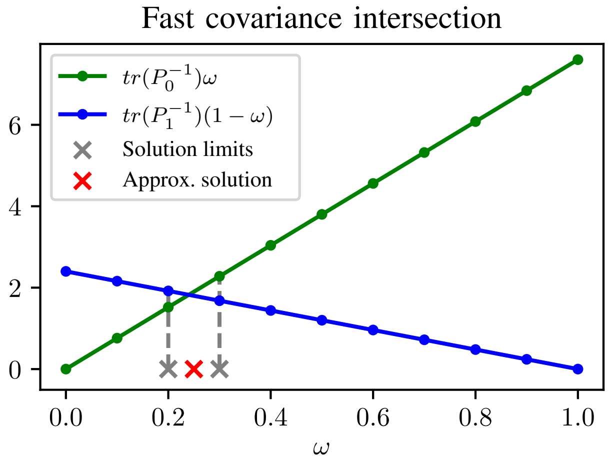

Fig. 1. Approximation of ω_0 with discretisation step size $s = 0.1$. Only comparisons of the ordered values sent from either estimator are used.

- 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 (25).
- 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.

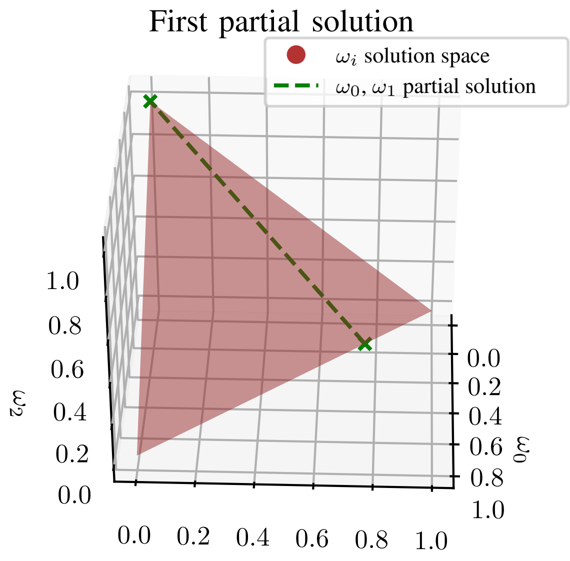

Fig. 2. Partial solution from equation (26) plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

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

V. Multi-Sensor Secure Fast Covariance Intersection

- In the multi sensor case, the same method of using PHE encryptions of each sensor's estimate and covariance is used to compute (1) and (2). Again we are left with the task of computing the weights ω_i.
- For the ease of diagrams we will demonstrate how this can be done in the three sensor case, and provide equations for the n sensor case.
- Computing the ω_i values for FCI in the three sensor case requires the solving of (26) and (27).

$$\omega_0\,\mathrm{tr}(\mathbf{P}_0) - \omega_1\,\mathrm{tr}(\mathbf{P}_1) = 0 \tag{26}$$
$$\omega_1\,\mathrm{tr}(\mathbf{P}_1) - \omega_2\,\mathrm{tr}(\mathbf{P}_2) = 0 \tag{27}$$

- Our method solves the multiple equations by approximating the partial solutions of each, similarly to the two sensor case, and solving the newly obtained, unencrypted, multiple equations.
- Partial solutions are treated as hyperplanes on the possible solutions space, and their intersection gives the solution to the mujltiple equations. We consider each ω_i a dimension, and defined hyperplane points as $(\omega_0, \omega_1, \ldots, \omega_n)$ accordingly.
- Solving (26) as was done in the two sensor case with (23) and (24), gives the partial solution of (26) when $\omega_2 = 0$ in the three sensor case. The other defining points of the partial solution of ω_0 and ω_1 are obtained when each remaining $\omega_i = 1$. In the three sensor case, this gives one aditional point; (0,0,1). In Fig. 2 the partial solution of (26) has been plotted over the solution space defined by (4) and (5) when $n = 2$.

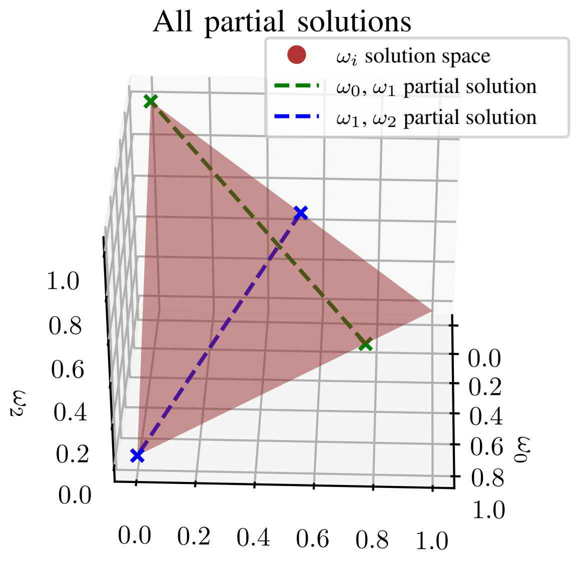

Fig. 3. Partial solutions from equations (26) and (27) plotted on the plane of all possible values of ω_0, ω_1, and ω_2.

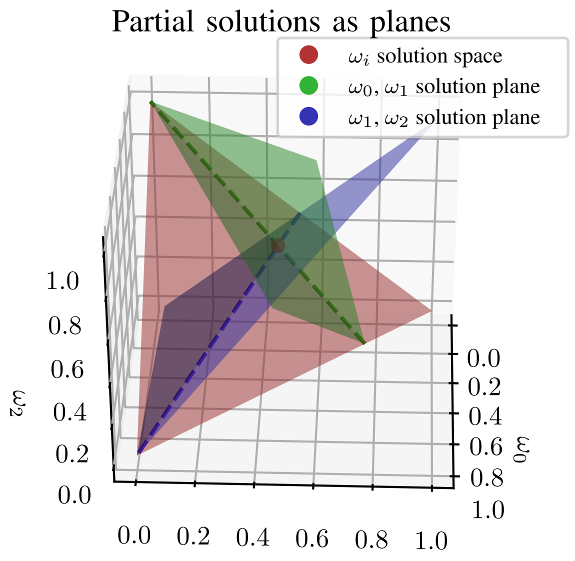

Fig. 4. Partial solutions from fig. 3 plotted as planes perpendicular to the plane of possible solutions. Intersection point gives solution values of ω_i for Fast Covariance Intersection.

- Next we compute the partial solution for ω_1, and ω_2 in the same way. The additional known point defining this partial solution space is $(1, 0, 0)$. Fig 3 shows both partial solutions plotted over the solution space. Note that the intersection of the partial solutions gives the approximate solution for the FCI ω values.

- The partial solutions provide $n-1$ hyperplanes, each of dimension $n-2$. When computing the partial solutions' intersection, we define hyperplanes of dimension $n-1$ for each partial solution, by adding a dimension perpendicular to the solution space. This can be seen in Fig. 4.

- Each partial solution in the three sensor case is therefore now defined as a plane of the form (28), where x, y, z represent the $\omega_0, \omega_1, \omega_2$ axes.

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

- We now have n equations, one of which is the solution space equation, and n values of $'omega_i$ to solve for. In the three sensor case, the solution to the linear problem (29) provides the approximate solution to each ω_i value in FCI.

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

- In the case of n sensors, hyperplanes are defined similarly, and produce the linear equation (30).

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

- Each of the partial solutions is approximated using consecutive sensor lists encrypted with ORE. This allows "Left-Right" ORE to still be used, by alternating which sensor uses which encryption.
- The required ordered lists sent from each sensor i are described by (31).

$$\begin{aligned} &[\mathcal{E}_{ORE}^{L}(\omega \operatorname{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is even} \\ &[\mathcal{E}_{ORE}^{R}(\omega \operatorname{tr}(\mathbf{P}_i^{-1})),\ \omega \in [0, 0+s, \ldots, 1-s, 1]],\ i \text{ is odd} \end{aligned} \tag{31}$$

VI. Simulation Results

- A simulation was implemented to demonstrate the accuracy of SecFCI fusion when compared to traditional FCI fusion.
- A constant-speed linear process model was used, with two independant cartesion sensors making white Gaussian noisy measurements of the ground truth. Both sensors ran linear Kalman Filters [] on their own measumrents producing a local estimate and estimate covariance.
- Sensors provided their estimates to a fusion center both in unencrypted form, and encrypted form. Unencrypted estimates consisted of only the estimates $\underline{\hat{x}}_i$ and $\mathbf{P}_i$, while encrypted estimates were composed of PHE encryption of the estimate in the information filter form, $\mathcal{E}(\mathbf{P}_i^{-1})$ and $\mathcal{E}(\mathbf{P}_i^{-1}\underline{\hat{x}}_i)$, and the ordered ORE encryptions defined in (31).

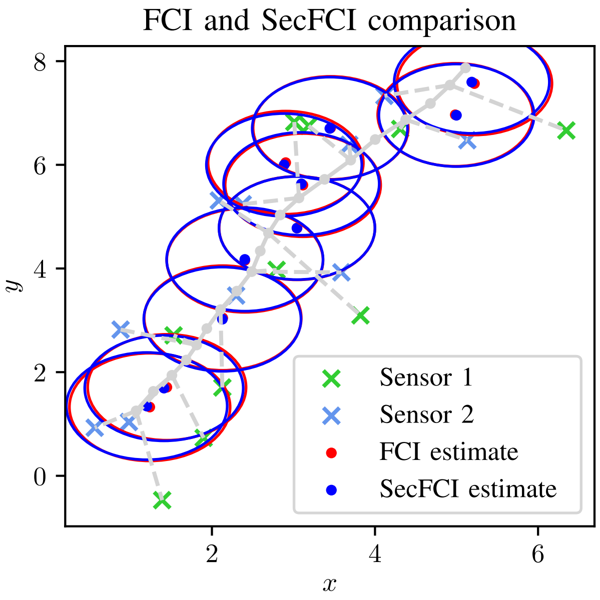

Fig. 5. Tracking simulation comparing Fast Covariance Intersection and our Secure Fast Covariance Intersection fusion methods.

- The fusion center then performed FCI fusion on the unencrypted estimates and our SecFCI fusion on the encrypted information. A portion of the trajectory and fused estimates are shown in Fig. 5.
- Fig. 6 plots the resulting fused estimate covariances' traces over the course of the simulation. Approximatation of exact FCI fusion results in slightly differing covariance traces as expected. In our simulation the resulting covariance trace of the SecFCI fusion algorithm is consistently higher than that of FCI fusion. However, this is not always the case, due to FCI itself computing an approximation to the trace minimising choice of ω.
- In Fig. 7 FCI and SecFCI values for each ω_i are plotted over the duration of a portion of the trajectory. SecFCI values for ω_i stay constant over time as can be expected due to the discretisation of partial solution estimates.

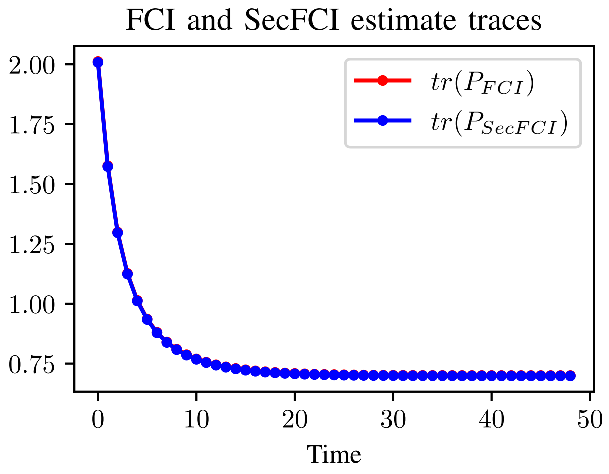

Fig. 6. Plot showing the fused estimate covariance trace throughout a tracking simulation, for both Fast Covariance Intersection and our Secure Fast Covariance Intersection

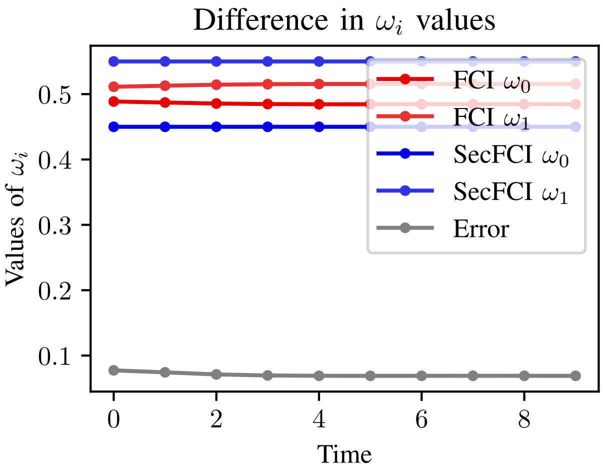

Fig. 7. Plot showing the difference in ω_i values between Fast Covariance Intersection and our Secure Fast Covariance Intersection, throughout a tracking simulation.

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.