

Dissertation for the Faculty of Computer Science (FIN),  
Otto von Guericke University (OVGU), Magdeburg

# **Data Confidentiality for Distributed Sensor Fusion**

Marko Ristic

September 29, 2022

Reviewers:

Prof. Dr.-Ing. Benjamin Noack (OVGU, Magdeburg, Germany)

...

# Contents

<b>Acknowledgements</b>	<b>iii</b>
<b>Abstract</b>	<b>iv</b>
<b>Kurzfassung</b>	<b>v</b>
<b>Notation</b>	<b>vi</b>
<b>1. Introduction</b>	<b>1</b>
1.1. State-of-the-Art and Research Questions . . . . .	2
1.2. Contributions . . . . .	3
1.3. Thesis Structure . . . . .	3
<b>2. Preliminaries</b>	<b>4</b>
2.1. Estimation Preliminaries . . . . .	4
2.1.1. Kalman Filter . . . . .	4
2.1.2. Kalman Filter Optimality . . . . .	4
2.1.3. Extended Kalman Filter . . . . .	4
2.1.4. Information Filter . . . . .	4
2.1.5. Extended Information Filter . . . . .	4
2.1.6. Fast Covariance Intersection . . . . .	4
2.2. Encryption Preliminaries . . . . .	5
2.2.1. Meeting Cryptographic Notions . . . . .	5
2.2.2. Paillier Homomorphic Encryption Scheme . . . . .	5
2.2.3. Joye-Libert Aggregation Scheme . . . . .	6
2.2.4. Lewi Order-Revealing Encryption Scheme . . . . .	7
2.2.5. Encoding Numbers for Encryption . . . . .	8
<b>3. Estimate Fusion on an Untrusted Cloud</b>	<b>10</b>
3.1. Problem Formulation . . . . .	10
3.2. Related Literature . . . . .	10
3.3. Confidential Cloud Fusion Leaking Fusion Weights . . . . .	10
3.4. Confidential Cloud Fusion Without Leakage . . . . .	10
3.5. Conclusions . . . . .	10
<b>4. Distributed Non-Linear Measurement Fusion with Untrusted Participants</b>	<b>11</b>
4.1. Problem Formulation . . . . .	11
4.2. Related Literature . . . . .	11

## Contents

4.3. Confidential Range-Only Localisation . . . . .	11
4.3.1. Unidirectional Alternative . . . . .	11
4.3.2. Solvable Sub-Class of Non-Linear Measurement Models . . . . .	11
4.4. Conclusions . . . . .	11
<b>5. Provable Estimation Performances</b>	<b>12</b>
5.1. Problem Formulation . . . . .	12
5.2. Related Literature . . . . .	12
5.3. Covariance Privilege . . . . .	12
5.4. Privileged Estimation for Linear Systems . . . . .	12
5.4.1. Extension to Non-Linear Systems . . . . .	12
5.5. Fusion in Privileged Estimation Environments . . . . .	12
5.6. Conclusions . . . . .	12
<b>6. Conclusion</b>	<b>13</b>
<b>A. Linear-Combination Aggregator Obliviousness</b>	<b>14</b>
<b>B. Cryptographic Proof of LCAO Scheme Security</b>	<b>15</b>

# Acknowledgements

Acks go here.

# Abstract

Distributed sensing and fusion algorithms are increasingly present in public computing networks and have led to a natural concern for data security in these environments. This thesis aims to present generalisable data fusion algorithms that simultaneously provide strict cryptographic guarantees on user data confidentiality. While fusion algorithms providing some degrees of security guarantees exist, these are typically either provided at the cost of solution generality or lack formal security proofs. Here, novel cryptographic constructs and state-of-the-art encryption schemes are used to develop formal security guarantees for new and generalised data fusion algorithms. Industry-standard Kalman filter derivatives are modified and existing schemes abstracted such that novel cryptographic notions capturing the required communications can be formalised, while simulations provide an analysis of practicality. Due to the generality of the presented solutions, broad applications are supported, including autonomous vehicle communications, smart sensor networks and distributed localisation.

# Kurzfassung

German abs go here.

# Notation

Complete the notation here.

# 1. Introduction

Sensor data processing, state estimation and data fusion have long been active areas of research and continue to find applications in modern systems [1, 2]. As distributed networks have become more prevalent over the years, greater stress has been put on the need for broadly applicable algorithms that support varying types of measurements, estimate accuracies and communication availabilities [3, 4], finding uses in localisation, weather forecasting, mapping, cooperative computing and cloud computing []. The use of Bayesian estimation methods such as the popular Kalman filter and its non-linear derivatives have become especially prevalent in application due to their recursive, often optimal, estimation properties and their suitability for modelling cross-correlations between local estimates [5, 6]. The handling of these cross-correlations, especially when they are not known in advance, is a common difficulty in state estimation and is tied to the challenges within the field [7]. The methods presented in this thesis and much of the related work in data fusion tasks similarly require the consideration of these challenges.

While the challenges relating to correlation errors are a well-established field of research, widespread advancements in distributed computing and uses of public networks for sensor communication have put a focus on the additional requirements of data privacy and state secrecy in recent years as well [8, 9]. Problems that require both the handling of correlation errors and guaranteeing a level of security for the participants involved are therefore a relevant topic in state estimation today and at the core of the work presented in this thesis. Achieving cryptographic secrecy typically involves hiding transferred information from unauthorised parties and can often be achieved irrespective of the estimation algorithms used by using common symmetric and public-key encryption schemes such as the Advanced Encryption Standard (AES) [10] and the Rivest-Shamir-Adleman cryptosystem (RSA) [11], respectively. These scenarios, however, imply a trust between encrypting and decrypting parties, which cannot always be assumed in distributed environments. In addition, partial computations on encrypted data or the intended leakage of some results are sometimes required for computing final results. This has led to several operation-providing and leakage-supporting encryption schemes [12, 13, 14, 15, 16] suitable for these distributed environments or when fine control over leakage is required. While these cryptographic schemes and notations are applicable in estimation and fusion tasks, the nature of cryptographic analysis in distributed environments, heavily dependent on communication protocols, has meant that developed solutions are often very context-specific, leading to numerous solutions for various estimation scenarios, use-cases and security requirements. This leads us to the current state-of-the-art literature on security-oriented state estimation and data fusion, observable gaps in this literature and the research questions we aim to answer.



## 1.1. State-of-the-Art and Research Questions

To summarise relevant work in security-oriented state estimation and data fusion we first discuss the security and types of data explored in this thesis. Regarding algorithms, we primarily consider stochastic models and outputs. As discussed in section [], Bayesian estimation methods such as the Kalman filter are prevalent due to their applicability and suitability for modelling phenomena accurately. In terms of security, we restrict ourselves to the data confidentiality component of the Confidentiality-Integrity-Availability (CIA) triad []. That is, the primary concern of security in this thesis is that concrete data deemed to be private to some participants remain so and its leakage is formally quantifiable. Data privacy, a related concept, is concerned with stopping the identification of individuals from available information. Although data privacy encompasses data confidentiality, it is a broader topic including communication traffic analyses and external cross-referencing to identify individuals and is not considered in its entirety in this thesis. That said, the terms *data privacy* and *privacy-preserving* are often used in the state-of-the-art to refer to data confidentiality alone and the ability to identify individuals from concrete data available []. The terms will be similarly used throughout this thesis.

Since knowing exact communications between participating parties is required for meaningful cryptographic analysis of transferred data, many existing general estimation algorithms have been restricted in some way to make communication and security easier to discuss. For example, [aristov] presents a distributed Kalman filter, namely an Information filter, where sensor measurements and measurement errors are known only to the measuring sensors while final estimates are leaked to an estimator. The restriction for this to be achieved requires sensors to form a hierarchical communication structure and measurement models to be linear, limiting the otherwise broadly applicable non-linear models or arbitrary communication structures. Another work, [proloc], presents localisation using range-only measurements where measurements and sensor locations, both required for localisation, are kept private to sensors and a centralised estimator while final estimates are available to an external trusted party. Here, no communication structure is enforced but produced estimates provide no error statistics and do not consider a dynamic process model.

In [pwsac, pwsah],  
aggregation papers  
differential privacy and differentially private Kalman filtering  
privacy-preserving optimisation with security based on statistical estimation  
added noise estimation  
—  
privacy-preserving image-based localisation  
eavesdropper paper with a secure return channel and a lossier channel for eavesdroppers  
GPS  
chaotic system paper  
physical layer noise paper (similar to chaotic noise paper)

## 1. Introduction

—

The two different approaches, restricting existing broad estimation methods in some ways to make cryptographic analysis plausible and ignoring formal security when assumptions and conclusions are intuitive demonstrate a gap in the existing literature and bring us to the target research topics this thesis aims to explore.

- dot point topics

These broad topics aim to fulfil the goal of generalisable but cryptographically provable estimation and fusion methods in distributed environments and lead to the concrete problems tackled in this work

### 1.2. Contributions

The contributions tackle the research topics in section .. by considering three concrete problems that coincide with the broader problems in the field

### 1.3. Thesis Structure

Each chapter includes relevant related literature to the specific problem and a formal problem formalisation before presenting the novel solutions.

## 2. Preliminaries

When introducing the novel estimation and cryptographic methods in this thesis, we make use of several existing algorithms. In this section, an overview of these methods is given

### 2.1. Estimation Preliminaries

As introduced in section ., the estimation and fusion algorithms considered are Bayesian and based on the Kalman filter and derivatives. The linear KF and linearising EKF are used explicitly and are the focus of the presented preliminaries.

#### 2.1.1. Kalman Filter

#### 2.1.2. Kalman Filter Optimality

#### 2.1.3. Extended Kalman Filter

#### 2.1.4. Information Filter

#### 2.1.5. Extended Information Filter

#### 2.1.6. Fast Covariance Intersection

Covariance Intersection (CI), introduced in [julierNondivergentEstimationAlgorithm1997], provides a consistent state estimate fusion algorithm when cross-correlations are not known. The resulting fused estimate  $\hat{\underline{x}}$  and covariance  $\mathbf{P}$  can be easily derived from its equations

$$\mathbf{P}^{-1} = \sum_{i=1}^n \omega_i \mathbf{P}_i^{-1}, \quad \mathbf{P}^{-1} \hat{\underline{x}} = \sum_{i=1}^n \omega_i \mathbf{P}_i^{-1} \underline{\hat{x}}_i . \quad (2.1)$$

Note that (2.1) computes the fusion of the information vectors and information matrices defined in [niehsenInformationFusionBased2002] and reduces the fusion to a weighted sum. Values for weights  $\omega_i$  must satisfy

$$\omega_1 + \omega_2 + \dots + \omega_n = 1, \quad 0 \leq \omega_i \leq 1 , \quad (2.2)$$

which guarantees consistency of the fused estimates. They are chosen in a way to speed up convergence and minimize the error by minimizing a certain specified property of the resulting fused estimate covariance. One such property, the covariance trace, requires

## 2. Preliminaries

the solution to

$$\arg \min_{\omega_1, \dots, \omega_n} \{\text{tr}(\mathbf{P})\} = \arg \min_{\omega_1, \dots, \omega_n} \left\{ \text{tr} \left( \left( \sum_{i=1}^n \omega_i \mathbf{P}_i^{-1} \right)^{-1} \right) \right\} \quad (2.3)$$

for computing weights  $\omega_i$ . However, minimizing this non-linear cost function can be very computationally costly and has led to the development of faster approximation techniques.

The Fast Covariance Intersection (FCI) algorithm from [niehsenInformationFusion-Based2002] is a non-iterative method for approximating the solution to (2.3) without the loss of guaranteed consistency. It is computed by defining a new constraint

$$\omega_i \text{tr}(\mathbf{P}_i) - \omega_j \text{tr}(\mathbf{P}_j) = 0, \quad i, j = 1, 2, \dots, n \quad (2.4)$$

on  $\omega_i$  and solving the resulting equations instead. In the two sensor case, this results in the solving of

$$\omega_1 \text{tr}(\mathbf{P}_1) - \omega_2 \text{tr}(\mathbf{P}_2) = 0, \quad \omega_1 + \omega_2 = 1 \quad (2.5)$$

When computed for  $n$  sensors, the highly redundant (2.4) can have its largest linearly independent subset represented by

$$\omega_i \text{tr}(\mathbf{P}_i) - \omega_{i+1} \text{tr}(\mathbf{P}_{i+1}) = 0, \quad i = 1, 2, \dots, n-1, \quad (2.6)$$

and requires the solution to the linear problem

$$\begin{bmatrix} \mathcal{P}_1 & -\mathcal{P}_2 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \mathcal{P}_{n-1} & -\mathcal{P}_n \\ 1 & \dots & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \omega_1 \\ \vdots \\ \omega_{n-1} \\ \omega_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}, \quad (2.7)$$

where we let  $\mathcal{P}_i = \text{tr}(\mathbf{P}_i)$ .

Our proposed filter aims to solve FCI fusion, namely (2.1) and (2.7), using only encrypted values from each sensor  $i$ , and leaking only the weight values  $\omega_1, \dots, \omega_n$ .

## 2.2. Encryption Preliminaries

Used cryptographic notions and schemes are summarised here. In addition, the encoding of floating point numbers to integers suitable for encryption by the presented schemes is introduced as well.

### 2.2.1. Meeting Cryptographic Notions

### 2.2.2. Paillier Homomorphic Encryption Scheme

The Paillier encryption scheme [paillierPublicKeyCryptosystemsBased1999] is an additively homomorphic encryption scheme that bases its security on the decisional composite

## 2. Preliminaries

residuosity assumption (DCRA) and meets the security notion of IND-CPA. Key generation of the Paillier scheme is performed by choosing two sufficiently large primes  $p$  and  $q$ , and computing  $N = pq$ . A generator  $g$  is also required for encryption, which is often set to  $g = N + 1$  when  $p$  and  $q$  are of equal bit length [katzIntroductionModernCryptography2008]. The public key is defined by  $(N, g)$  and the secret key by  $(p, q)$ .

Encryption of a plaintext message  $a \in \mathbb{Z}_N$ , producing ciphertext  $c \in \mathbb{Z}_{N^2}^*$ , is computed by

$$c = g^a \rho^N \pmod{N^2} \quad (2.8)$$

for a randomly chosen  $\rho \in \mathbb{Z}_N$ . Here,  $\rho^N$  can be considered the noise term which hides the value  $g^a \pmod{N^2}$ , which due to the scheme construction, is an easily computable discrete logarithm. The decryption of a ciphertext is computed by

$$a = \frac{L(c^\lambda \pmod{N^2})}{L(g^\lambda \pmod{N^2})} \pmod{N} \quad (2.9)$$

where  $\lambda = \text{lcm}(p-1, q-1)$  and  $L(\psi) = \frac{\psi-1}{N}$ .

In addition to encryption and decryption, the following homomorphic functions are provided by the Paillier scheme.  $\forall a_1, a_2 \in \mathbb{Z}_N$ ,

$$\mathcal{D}(\mathcal{E}(a_1)\mathcal{E}(a_2) \pmod{N^2}) = a_1 + a_2 \pmod{N}, \quad (2.10)$$

$$\mathcal{D}(\mathcal{E}(a_1)g^{a_2} \pmod{N^2}) = a_1 + a_2 \pmod{N}, \quad (2.11)$$

$$\mathcal{D}(\mathcal{E}(a_1)^{a_2} \pmod{N^2}) = a_1 a_2 \pmod{N}. \quad (2.12)$$

### 2.2.3. Joye-Libert Aggregation Scheme

The Joye-Libert privacy-preserving aggregation scheme [joyeScalableSchemePrivacyPreserving2013] is a scheme defined on time-series data and meets the security notion of Aggregator Obliviousness (AO) [shiPrivacyPreservingAggregationTimeSeries2011]. Similarly to the Paillier scheme, it bases its security on the DCRA. A notable difference to a public-key encryption scheme is its need for a trusted party to perform the initial key generation and distribution.

Key generation is computed by first choosing two equal-length and sufficiently large primes  $p$  and  $q$ , and computing  $N = pq$ . A hash function  $H : \mathbb{Z} \rightarrow \mathbb{Z}_{N^2}^*$  is defined and the public key is set to  $(N, H)$ .  $n$  private keys are generated by choosing  $sk_i, i \in \{1, \dots, n\}$ , uniformly from  $\mathbb{Z}_{N^2}$  and distributing them to  $n$  participants (whose values are to be aggregated), while the last key is set as

$$sk_0 = - \sum_{i=1}^n sk_i, \quad (2.13)$$

and sent to the aggregator.

Encryption of plaintext  $a_i^{(t)} \in \mathbb{Z}_N$  to ciphertext  $c_i^{(t)} \in \mathbb{Z}_{N^2}$  at instance  $t$  is computed by user  $i$  as

$$c_i^{(t)} = (N+1)^{a_i^{(t)}} H(t)^{sk_i} \pmod{N^2}. \quad (2.14)$$

## 2. Preliminaries

Here, we can consider  $H(t)^{sk_i}$  the noise term which hides the easily computable discrete logarithm  $g^{a_i^{(t)}} \pmod{N^2}$ , where  $g = N + 1$  (as with the Paillier scheme above).

When all encryptions  $c_i^{(t)}$ ,  $i \in \{1, \dots, n\}$  are sent to the aggregator, summation and decryption of the aggregated sum are computed by the functions

$$c^{(t)} = H(t)^{sk_0} \prod_{i=1}^n c_i^{(t)} \pmod{N^2} \quad (2.15)$$

and

$$\sum_{i=1}^n a_i^{(t)} = \frac{c^{(t)} - 1}{N} \pmod{N}. \quad (2.16)$$

Correctness follows from  $\sum_{i=0}^n sk_i = 0$ , and thus

$$\begin{aligned} & H(t)^{sk_0} \prod_{i=1}^n c_i^{(t)} \pmod{N^2} \\ & \equiv H(t)^{sk_0} \prod_{i=1}^n (N + 1)^{a_i^{(t)}} H(t)^{sk_i} \pmod{N^2} \\ & \equiv H(t)^{\sum_{j=0}^n sk_j} \prod_{i=1}^n (N + 1)^{a_i^{(t)}} \pmod{N^2} \\ & \equiv (N + 1)^{\sum_{i=1}^n a_i^{(t)}} \pmod{N^2}, \end{aligned}$$

removing all noise terms.

### 2.2.4. Lewi Order-Revealing Encryption Scheme

For ORE, we use the Lewi symmetric-key Left-Right ORE scheme as it has the added property of only allowing certain comparisons between cyphertexts. This property can be used to decide which values may not be compared, which will be shown in the section ... It is described as follows: two encryption functions allow integers to be encrypted as either a “Left” ( $L$ ) or “Right” ( $R$ ) encryption by

$$\begin{aligned} \text{enc}_{\text{ORE}}^L(k, x) &= \mathcal{E}_{\text{ORE}, k}^L(x), \\ \text{enc}_{\text{ORE}}^R(k, y) &= \mathcal{E}_{\text{ORE}, k}^R(y), \end{aligned} \quad (2.17)$$

and only comparisons between an  $L$  and an  $R$  encryption are possible, by

$$\text{cmp}_{\text{ORE}}(\mathcal{E}_{\text{ORE}}^L(x), \mathcal{E}_{\text{ORE}}^R(y)) = \text{cmp}(x, y). \quad (2.18)$$

Note that no decryption function is provided as only encryptions are required to provide a secure comparison. The Lewi ORE encryption scheme provides security against the simulation-based security model [chenettePracticalOrderRevealingEncryption2016] but is not secure against the IND-OCPA model.

### 2.2.5. Encoding Numbers for Encryption

In both the Paillier and Joye-Libert schemes, as well as the one we introduce, meaningful inputs  $a$  are bounded to  $a \in \mathbb{Z}_N$ . For this reason, real-valued estimation variables require quantisation and integer mapping for encryption and aggregation. We will rely on a generalised Q number encoding [oberstarFixedPointRepresentationFractional2007] due to implementation simplicity and applicability.

We will consider a subset of rational numbers in terms of a range  $M \in \mathbb{N}$  and fractional precision  $\phi \in \mathbb{N}$ . This contrasts with the common definition in terms of total and fractional bits [oberstarFixedPointRepresentationFractional2007, schulzedarupEncryptedCooperativeControl2019, farokhiSecurePrivateControl2017], but allows for a direct mapping to integer ranges which are not a power of two. A rational subset  $\mathbb{Q}_{M,\phi}$  is then given by

$$\mathbb{Q}_{M,\phi} = \left\{ o \mid \phi o \in \mathbb{N} \wedge -\left\lfloor \frac{M}{2} \right\rfloor \leq \phi o < \left\lfloor \frac{M}{2} \right\rfloor \right\}, \quad (2.19)$$

and we can quantize any real number  $a$  by taking the nearest rational  $o \in \mathbb{Q}_{M,\phi}$ , that is,  $\arg \min_{o \in \mathbb{Q}_{M,\phi}} |a - o|$ . In this form, mapping rationals  $\mathbb{Q}_{M,\phi}$  to an encryption range  $\mathbb{Z}_N$  is achieved by choosing  $M = N$  and handling negatives by modulo arithmetic. Additionally, we note that the Q number format requires a precision factor  $\phi$  to be removed after each encoded multiplication. This is captured by a third parameter  $d$ ; the number of additional precision factors present in encodings.

The function for *combined* quantisation and encoding,  $E_{M,\phi,d}(a)$ , of a given number  $a \in \mathbb{R}$  and with an integer range  $\mathbb{Z}_M$ , precision  $\phi$  and scaling for  $d$  prior encoded multiplications is given by

$$E_{M,\phi,d}(a) = \left\lfloor \phi^{d+1} a \right\rfloor \pmod{M}. \quad (2.20)$$

Decoding of an integer  $u \in \mathbb{Z}_M$ , is given by

$$E_{M,\phi,d}^{-1}(u) = \begin{cases} \frac{u \pmod{M}}{\phi^{d+1}}, & u \pmod{M} \leq \left\lfloor \frac{M}{2} \right\rfloor \\ -\frac{M - u \pmod{M}}{\phi^{d+1}}, & \text{otherwise} \end{cases}. \quad (2.21)$$

This encoding scheme provides the following homomorphic operations,

$$E_{M,\phi,d}(a_1) + E_{M,\phi,d}(a_2) \pmod{M} = E_{M,\phi,d}(a_1 + a_2) \quad (2.22)$$

and

$$E_{M,\phi,d}(a_1) E_{M,\phi,d}(a_2) \pmod{M} = E_{M,\phi,d+1}(a_1 a_2), \quad (2.23)$$

noting that when  $M = N$ , the operations and modulus correspond with those in the Paillier homomorphic operations (2.10), (2.11) and (2.12), and the Joye-Libert sum (2.16).

## 2. Preliminaries

In general, the choice of a large precision parameter  $\phi$  may reduce quantisation errors introduced in (2.20), but risks overflow after too many multiplications. Given the largest number of encoded multiplications,  $d_{max}$ , and the largest value to be encoded  $a_{max}$ , the parameter should be chosen such that

$$\left| \phi^{d_{max}+1} a_{max} \right| < \left\lfloor \frac{M}{2} \right\rfloor. \quad (2.24)$$

In practice,  $N$  is typically very large ( $N > 2^{1024}$ ) and this condition can be ignored when  $M = N$ , as  $\phi$  can be made sufficiently large to make quantisation errors negligible.



## **3. Estimate Fusion on an Untrusted Cloud**

### **3.1. Problem Formulation**

### **3.2. Related Literature**

### **3.3. Confidential Cloud Fusion Leaking Fusion Weights**

### **3.4. Confidential Cloud Fusion Without Leakage**

### **3.5. Conclusions**

## **4. Distributed Non-Linear Measurement Fusion with Untrusted Participants**

### **4.1. Problem Formulation**

### **4.2. Related Literature**

### **4.3. Confidential Range-Only Localisation**

#### **4.3.1. Unidirectional Alternative**

#### **4.3.2. Solvable Sub-Class of Non-Linear Measurement Models**

### **4.4. Conclusions**

## **5. Provable Estimation Performances**

### **5.1. Problem Formulation**

### **5.2. Related Literature**

### **5.3. Covariance Privilege**

### **5.4. Privileged Estimation for Linear Systems**

#### **5.4.1. Extension to Non-Linear Systems**

### **5.5. Fusion in Privileged Estimation Environments**

### **5.6. Conclusions**

## **6. Conclusion**

## **A. Linear-Combination Aggregator Obliviousness**

## **B. Cryptographic Proof of LCAO Scheme Security**

## List of Figures

## List of Tables



# Bibliography

- [1] B. D. O. Anderson and J. B. Moore, *Optimal Filtering*. Dover Publications, 1979.
- [2] D. Simon, *Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches*. John Wiley & Sons, 2006.
- [3] A. G. O. Mutambara, *Decentralized Estimation and Control for Multisensor Systems*. CRC press, 1998.
- [4] M. Liggins, C. Y. Chong, D. Hall, and J. Llinas, *Distributed Data Fusion for Network-Centric Operations*. CRC Press, 2012.
- [5] C. Y. Chong, “Forty Years of Distributed Estimation: A Review of Noteworthy Developments,” in *IEEE ISIF Workshop on Sensor Data Fusion: Trends, Solutions, Applications (SDF 2017)*, 2017, pp. 1–10.
- [6] A. J. Haug, *Bayesian Estimation and Tracking: A Practical Guide*. John Wiley & Sons, 2012.
- [7] B. Noack, J. Sijs, M. Reinhardt, and U. D. Hanebeck, *Treatment of Dependent Information in Multisensor Kalman Filtering and Data Fusion*. CRC Press, 2017, pp. 169–192.
- [8] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith, “Secret Program Execution in the Cloud Applying Homomorphic Encryption,” in *5th IEEE International Conference on Digital Ecosystems and Technologies (DEST)*, 2011, pp. 114–119.
- [9] K. Ren, C. Wang, and Q. Wang, “Security Challenges for the Public Cloud,” *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.
- [10] S. Gueron, “Intel Advanced Encryption Standard (AES) New Instructions Set,” *Intel Corporation*, 2010.
- [11] R. L. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-key Cryptosystems,” *Communications of the ACM (CACM)*, vol. 21, no. 2, pp. 120–126, 1978.
- [12] P. Paillier, “Public-Key Cryptosystems Based on Composite Degree Residuosity Classes,” in *Advances in Cryptology (EUROCRYPT)*. Springer, 1999, pp. 223–238.

## Bibliography

- [13] E. Shi, T.-H. H. Chan, and E. Rieffel, “Privacy-Preserving Aggregation of Time-Series Data,” *Annual Network & Distributed System Security Symposium (NDSS)*, p. 17, 2011.
- [14] M. Joye and B. Libert, “A Scalable Scheme for Privacy-Preserving Aggregation of Time-Series Data,” in *International Conference on Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science. Springer, 2013, pp. 111–125.
- [15] J. Chotard, E. Dufour Sans, R. Gay, D. H. Phan, and D. Pointcheval, “Decentralized Multi-Client Functional Encryption for Inner Product,” in *Advances in Cryptology (ASIACRYPT)*, ser. Lecture Notes in Computer Science. Springer, 2018, pp. 703–732.
- [16] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, “Geo-Indistinguishability: Differential Privacy for Location-Based Systems,” in *ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS ’13. New York, NY, USA: Association for Computing Machinery, 2013, pp. 901–914.