Cryptographically Privileged State Estimation With Gaussian Keystreams

Marko Ristic
Intelligent Sensor-Actuator-Systems (ISAS)
Karlsruhe Institute of Technology (KIT), Germany
Email: marko.ristic@kit.edu

Benjamin Noack
Intelligent Sensor-Actuator-Systems (ISAS)
Karlsruhe Institute of Technology (KIT), Germany
Email: noack@kit.edu

Uwe D. Hanebeck
Intelligent Sensor-Actuator-Systems (ISAS)
Karlsruhe Institute of Technology (KIT), Germany
Email: uwe.hanebeck@kit.edu

***Abstract*—State estimation via public channels requires additional planning with regards to state privacy and the information leakage of involved parties. In some scenarios it is desirable to allow partial leakage of state information, thus distinguishing between privileged and unprivileged estimators and their capabilities. Existing methods identifying privileged and unprivileged or trusted and untrusted estimators typically result in reduced estimation quality for both parties or require additional secure channels of communication. We introduce a method to diminish the estimation quality at unprivileged estimators using a stream of pseudorandom Gaussian samples while leaving privileged estimation unaffected and requiring no additional transmission beyond an initial key exchange. A cryptographic definition of privileged estimation is first presented, capturing the definition of the difference between estimation qualities, before we develop a Gaussian keystream privileged estimation scheme meeting the security criteria defined. Achieving privileged estimation without additional channel requirements allows quantifiable estimation to be made available to the public while keeping the best estimation private to trusted privileged parties and can find uses in a variety of service providing and privacy-preserving scenarios.**

I. Introduction

The role of state estimation and sensor data processing has become increasingly prevalent in modern systems [1]. Particularly, since the development of Kalman estimation theory, Bayesian state estimation has found common application, varying from autonomous systems to remote estimation [2], [3]. As advancements in distributed algorithms and cloud computing develop, the use of wireless and public communication channels for data transmission has become widespread, bringing to light the requirements of data privacy and state secrecy [4], [5].

Typically, use-cases for preserving data privacy over public channels involve hiding all transferred information such that eavesdroppers or present untrusted parties learn no additional information from the observed data. This is achievable using common encryption schemes such as AES [6] or RSA [7] which formally capture this security requirement by satisfying cryptographic ciphertext indistinguishability [8]. Some more advanced requirements using public channels also exist. When partial information needs to be made public, or computations need to be performed on data, homomorphic or aggregation encryption schemes can be used. [9] proposes localisation where individual sensors and measurements remain private using homomorphic encryption. [10] has distributed control inputs aggregated without parties learning individual contributions, while [11], [12] use homomorphic encryption to allow control inputs to be computed without decryption. In the context of estimation, a quantifiable difference in estimation performance between untrusted and trusted parties can provide different levels of estimation privilege. This was achieved in the initial release of the Global Positioning System (GPS) [13], which relied on a second, encrypted, stream of information required for accurate estimation. Another example is seen in [14], where intermittent sending is proposed to increase eavesdropper estimation error while using a secure feedback channel to ensure better estimation for trusted parties. Our contribution in this work considers this context of privileged and unprivileged estimation and is comprised of a formal definition of privileged state estimation, crucial for providing cryptographic security albeit often neglected, before proposing an estimation scheme which provides privileged levels of estimation without reliance on additional secure channels or privileged estimator feedback. We accompany the method with a cryptographic proof sketch and simulation results.

In section II we introduce the relevant privileged estimation problem followed by a cryptographic formalisation of desired properties. Section III introduces our proposed privileged estimation scheme and in section IV a cryptographic proof sketch is given. A simulation of the method is then demonstrated and explained in section V, while concluding remarks and future work are discussed in section VI.

A. Notation

Throughout this work the following notation is used. Lowercase underlined characters $\underline{a}$ denote vectors, while uppercase bold characters $\mathbf{M}$ denote matrices. $\mathbf{M} \succ 0$ and $\mathbf{M} \succeq 0$ denote positive definitiveness and positive semi-definitiveness, respectively, and $\mathbf{M} \succ \mathbf{N}$ is used as shorthand for $\mathbf{M}-\mathbf{N} \succ 0$. Function $\mathsf{eig}(\mathbf{M})$ gives the set of eigenvalues for matrix $\mathbf{M}$, $\mathsf{Cov}[\cdot]$ computes the covariance of a random vector and $\mathbf{I}$ is the identity matrix with size inferrable from context.

II. Problem Statement

We consider the estimation scenario where process and measurement models are known, and state estimators are either privileged estimators possessing a secret key or unprivileged estimators without. We aim to develop a scheme for which the difference in their estimation errors is quantifiable and cryptographically guaranteed when process and measurement models are Gaussian, linear and time-invariant.

The process model we consider gives the state $\underline{x}_k \in \mathbb{R}^n$ at a time k and is given by

$$\underline{x}_k = \mathbf{F}\underline{x}_{k-1} + \underline{w}_k\,, \tag{1}$$

with noise term $\underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q})$ and a known covariance $\mathbf{Q} \in \mathbb{R}^{n\times n}$. Similarly, the measurement model gives the measurement $\underline{y}_k$ at time k and is given by

$$\underline{y}_k = \mathbf{H}\underline{x}_k + \underline{v}_k\,, \tag{2}$$

with noise term $\underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R})$ and a known covariance $\mathbf{R} \in \mathbb{R}^{m\times m}$.

To capture our aim of creating a privileged and unprivileged estimator, we must first define how to assess the estimation advantage between estimators, and which algorithms are required to characterise a privileged estimation scheme. In the following section, we give relevant formal definitions, which will be used when assessing the security of our proposed scheme.

A. Formal cryptographic Problem

While we are interested in Gaussian, linear and time-invariant models, it is more practical to define a broader security notion that can be satisfied under arbitrary specified conditions on the models. This allows the use of the security notion in future literature and is more in-line with typical cryptographic practice. We will later show that our proposed scheme meets this security notion under the specific Gaussian, linear and time-invariant model assumptions.

Typical formal cryptographic security notions are given in terms of probabilistic polynomial-time (PPT) attackers and capture desired privacy properties as well as attacker capabilities [8]. The most commonly desired privacy property, cryptographic indistinguishability, is not suitable for our estimation scenario due to our desire for unprivileged estimators to gain some information from measurements. Instead, we will define security with respect to a time series of covariances, given arbitrary known Bayesian models, such that the difference in estimation error between estimators with and without the secret key is bounded by the series at all times.

To formalise this, we introduce the following notations and definitions. We assume the existence of an arbitrary process (not necessarily Gaussian or linear) following a known model exactly, with the state at time k denoted $\underline{x}_k \in \mathbb{R}^n$ and model parameters $\mathcal{M}_P$. Similarly, we assume the existence of a means of process measurement following a known measurement model exactly, with the measurement at time k denoted $\underline{y}_k \in \mathbb{R}^m$ and model parameters $\mathcal{M}_M$. We can now define a *privileged estimation scheme* as a pair of algorithms $(\mathsf{Setup}, \mathsf{Noise})$ given by

$\mathsf{Setup}(\mathcal{M}_P, \mathcal{M}_M, \kappa)$ On the input of models $\mathcal{M}_P$ and $\mathcal{M}_M$, and the security parameter κ, public parameters pub and a secret key sk are created.

$\mathsf{Noise}(\mathsf{sk}, k, \mathcal{M}_P, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k)$ On input of secret key sk, time k, models $\mathcal{M}_P$ and $\mathcal{M}_M$, and measaurements $y_1, \ldots, y_k$, a noisy measurement $\underline{y}'_k$ (with no required model constraints) is created.

In addition to the scheme description above, we also give the following definitions to help formalise our desired security notion.

Definition II.1. An *estimator* is any algorithm which produces a guess of the state $\underline{x}_k$ for a given time k.

Definition II.2. A *negligible covariance function* is a function

$$\mathsf{negl}\mathsf{Cov}_m(\kappa) : \mathbb{N} \to \mathbb{R}^{m\times m} \tag{3}$$

that returns a matrix $\mathbf{A}$ such that $\mathbf{A}$ is a valid covariance ($\mathbf{A} \succ 0$ and $\mathbf{A} = \mathbf{A}^\top$) and that for each of its eigenvalues $e \in \mathsf{eig}(\mathbf{A})$, there exists a negligible function η such that $e \leq \eta(\kappa)$.

With the terminology above, we can now introduce the security notion which captures the formal requirements of the estimation problem that we want to solve.

Definition II.3. A privileged estimation scheme meets notion $\{\mathbf{D}_1, \mathbf{D}_2, \ldots\}$-*Covariance Privilege for Models $\mathcal{M}_P$ and $\mathcal{M}_M$* if for any PPT estimator $\mathcal{A}$, there exists a PPT estimator $\mathcal{A}'$, such that

$$\begin{aligned}&\mathsf{Cov}\left[\mathcal{A}\left(k, \kappa, \mathsf{pub}, \mathcal{M}_P, \mathcal{M}_M, \underline{y}'_1, \ldots, \underline{y}'_k\right) - \underline{x}_k\right] \\ &- \mathsf{Cov}\left[\mathcal{A}'\left(k, \kappa, \mathsf{pub}, \mathcal{M}_P, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k\right) - \underline{x}_k\right] \\ &\succeq \mathbf{D}_k + \mathsf{negl}\mathsf{Cov}_m(\kappa)\end{aligned} \tag{4}$$

for valid covariances $\mathbf{D}_1, \mathbf{D}_2, \ldots$ and some negligible covariance for all $k > 0$. Here, estimators $\mathcal{A}$ and $\mathcal{A}'$ are running in polynomial-time with respect to the security parameter κ, and all probabilities are taken over models $\mathcal{M}_P$ and $\mathcal{M}_M$, estimators $\mathcal{A}$ and $\mathcal{A}'$, and algorithms Setup and Noise.

Informally, the above definition states that no estimator that can only access noisy measurements $\underline{y}'_1, \ldots, \underline{y}'_k$ can estimate a state $\underline{x}_k$ for a time k with a mean square error (MSE) covariance less than an equivalent estimator with access to true measurements $\underline{y}_1, \ldots, \underline{y}_k$, by a margin of at least $\mathbf{D}_k$. Next, we will propose a scheme meeting the aforementioned notion for a derivable series of covariances when models $\mathcal{M}_P$ and $\mathcal{M}_M$ are Gaussian, linear and time-invariant.

III. Privileged Estimation

The general idea behind our privileged estimation scheme is adding pseudorandom noise to measurements at the sensor, degrading the state estimation at estimators that cannot remove it. The added noise is a keystream generated from a secret key and can be generated and removed from measurements by any sensor holding the same key.

To allow meeting the cryptographic notion in section II-A we focus on Gaussian, linear and time-invariant models where the minimum achievable error covariance is easily computable, and produce a keystream of pseudorandom Gaussian noise. The keystream and added noise are given next.

A. Gaussian Keystream

To generate pseudorandom Gaussian samples, we rely on first generating a typical cryptographic pseudorandom bitstream given a secret key sk. Using a well-studied method for the generation of pseudorandomness guarantees robustness and easy updating should a used scheme no longer be considered safe. Any cryptographic stream cipher can be used and we interpret the bitstream as sequential pseudorandom integers $q_t \in \mathbb{N}$, $0 < t$, of a suitable size, and use them to generate a sequence of pseudorandom uniform real numbers $u_t \dot{\sim} \mathcal{U}(0,1)$.

The conversion of q_t to u_t is cryptographically non-trivial due to the floating-point representation of u_t. Since it cannot be truly representative of the distribution $\mathcal{U}(0,1)$, the pseudorandomness of samples is affected and meeting the desired cryptographic notion complicated. For now, we will assume that the uniform floating-point numbers are sufficiently close to true uniform reals, as is the current industry standard, and rely on any common method for choosing the bit size of integers q_t and the pseudorandom generation of uniforms u_t [15]. In section IV we will state and further discuss this assumption.

Given the sufficiently uniform pseudorandom floating-point numbers u_t, we are left with generating a series of pseudorandom standard normal Gaussian samples, which can be readily computed using the Box-Muller transform [16], by

$$z_t = \sqrt{-2\ln(u_t)}\cos(2\pi u_{t+1}) \tag{5}$$

and

$$z_{t+1} = \sqrt{-2\ln(u_t)}\sin(2\pi u_{t+1}) \tag{6}$$

to obtain two sequential, independent, standard normal Gaussian samples from two uniform ones. This Gaussian keystream can then be used by privileged estimation scheme to add arbitrary pseudorandom multivariate Gaussian noise.

B. Additional Gaussian Noise

To use the series of pseudorandom Gaussian samples z_t, $0 < t$, at the sensor and privileged estimator, they need to be converted to n-dimension zero-mean multivariate Gaussian samples suitable for use in the measurement model (2), at every time k. In addition, we want control over the difference in estimation error between privileged and unprivileged estimators, and do so by including the symettric matrix parameter $\mathbf{Z} \succ 0$, such that added pseudorandom noise $\underline{p}_k$ at time k is such that $\underline{p}_k \dot{\sim} \mathcal{N}(\underline{0}, \mathbf{Z})$. Given $\mathbf{Z}$, $\underline{p}_k$ is computed using the next n Gaussian keystream samples, that is $(k-1)n+1 \leq t \leq kn$, as

$$\underline{p}_k = \mathbf{Z} \cdot \begin{bmatrix} z_{(k-1)n+1} & \dots & z_{kn} \end{bmatrix}^\top . \tag{7}$$

Before estimation, we assume that the secret key sk, required for generating the Gaussian keystream in section III-A, has been shared between the sensor and privileged estimator. During estimation, the sensor modifies its measurements $\underline{y}_k$ by

$$\underline{y}'_k = \underline{y}_k + \underline{p}_k \,, \tag{8}$$

resulting in a new measurement model

$$\underline{y}'_k = \mathbf{H}\underline{x}_k + \underline{v}_k + \underline{p}_k \,, \tag{9}$$

with $\underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R})$ and $\underline{p}_k \dot{\sim} \mathcal{N}(\underline{0}, \mathbf{Z})$. There are now two estimation problems present for the privileged and unprivileged estimator respectively.

Privileged estimation The estimator that holds the secret key sk can compute the Gaussian key stream z_t, $0 < t$, and therefore added noise vectors $\underline{p}_k$ at every time k. Computing $\underline{y}_k = \underline{y}'_k - \underline{p}_k$ given the noisy measurements results in the original measurements following measurement model (2) exactly.

Unprivileged estimation In the case where pseudorandomness is indistinguishable from randomness, as is the case at an unprivileged estimator when using a cryptographically secure keystream and sk is not known, noisy measurements are indistinguishable from those following the modified measurement model

$$\underline{y}'_k = \mathbf{H}\underline{x}_k + \underline{v}'_k \,, \tag{10}$$

with $\underline{v}'_k \sim \mathcal{N}(\underline{0}, \mathbf{R}+\mathbf{Z})$, exactly.

Intuitively, we can see that the two estimators will have their difference in estimation error dependent on matrix $\mathbf{Z}$. In the security section, we will show that the best possible error covariances achievable by the privileged and unprivileged estimators can be computed exactly for both measurement models and that the difference between them will give the series $\{\mathbf{D}_1, \mathbf{D}_2, \dots\}$ required for the security notion (4).

C. Multiple Privileges

In the above scenario, we have considered a single level of estimation privileged with one private key, dividing estimation error covariance into two groups. As a direct extension, it may be desirable to define multiple *levels* of privilege, such that the best estimation performance depends on the privilege level of an estimator. Here we will briefly put forward one such example, where a single secret key corresponds to each privilege level and noise is added similarly to (8) for each key individually.

We now have N secret keys sk_i and covariances for the added noises $\mathbf{Z}_i$, $1 \leq i \leq N$. Sensor measurements are modified by

$$\underline{y}'_k = \underline{y}_k + \underline{p}_k^{(1)} + \dots + \underline{p}_k^{(N)} \,, \tag{11}$$

with $\underline{p}_k^{(i)} \dot{\sim} \mathcal{N}(\underline{0}, \mathbf{Z}_i)$, $1 \leq i \leq N$. From (11), we see that obtaining any single key sk_i leads to a measurement model where only a single pseudorandom Gaussian sample, of covariance

Z_i, is removed, resulting in measurements indistinguishable from those following the modified measurement model

$$\underline{y}'_k = \mathbf{H}\underline{x}_k + \underline{v}_k^{(i)}\,, \tag{12}$$

where $\underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R} + \mathbf{E}_i)$, with

$$\mathbf{E}_i = \sum_{j=1, j\neq i}^{N} \mathbf{Z}_j\,. \tag{13}$$

As values $\mathbf{E}_i$ directly correspond to the relative estimation performances of each privilege level, we are also interested in the numerical restrictions when choosing these matrices. For the models to be valid for any measurement covariance $\mathbf{R}$, it is clear that $\mathbf{E}_i \succ 0$ and $\mathbf{E} = \mathbf{E}^\top$ must hold for all $1 \leq i \leq N$, but due to the dependence of $\mathbf{Z}_i$ there is an additional restriction required to ensure all values of $\mathbf{Z}_i$ remain valid covariances as well. From (13) we can write

$$\begin{bmatrix} \mathbf{0} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} \\ \mathbf{I} & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{I} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{I} & \cdots & \mathbf{I} & \mathbf{0} & \mathbf{I} \\ \mathbf{I} & \cdots & \mathbf{I} & \mathbf{I} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \mathbf{Z}_1 \\ \mathbf{Z}_2 \\ \vdots \\ \mathbf{Z}_{N-1} \\ \mathbf{Z}_N \end{bmatrix} = \begin{bmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \\ \vdots \\ \mathbf{E}_{N-1} \\ \mathbf{E}_N \end{bmatrix}, \tag{14}$$

which, when rearranged and the conditions $\mathbf{Z}_i \succ 0$ are taken into account, gives the additional requirement

$$\mathbf{E}_i \prec \frac{1}{N-1} \sum_{j=1}^{N} \mathbf{E}_j \tag{15}$$

for all $1 \leq i \leq N$.

From (15) we can see that privilege levels are significantly restricted in relative estimation performance. We have demonstrated this method due to its simplicity and relation to the single level scheme, however, alternative methods involving multiple or overlapping keys may allow weaker restrictions and will be considered in future work.

IV. Scheme Security

The security of the proposed scheme will be primarily considered in the single privileged estimation level as introduced in section III-B and a proof sketch will be provided to show how the proposed scheme meets the cryptographic notion (4). The extension to multiple privilege levels as described in section III-C will be informally discussed afterwards.

A. Single Privileged Case

Recalling the security notion in section (2), we now aim to show how our single privilege level estimation scheme in section III-B, given conditions on $\mathcal{M}_P$ and $\mathcal{M}_M$, meets the notion for a computable series $\mathbf{D}_1, \mathbf{D}_2, \ldots$ dependent on the noise parameter $\mathbf{Z}$.

We consider the process model (1) and measurement model (2) exactly, that is, any time-invariant linear models with known zero-mean Gaussian additive noises. We define these are our model conditions and capture all relevant parameter from the respective equations in $\mathcal{M}_P$ and $\mathcal{M}_M$. Our scheme fulfils the two required algorithms for a privileged estimation scheme, Setup and Noise, as follows.

Setup Initialise a cryptographically indistinguishable stream cipher with the parameter κ, set the secret key sk to the stream cipher key and include initial filter estimate $\hat{\underline{x}}_0$, error covariance $\mathbf{P}_0$ and additional noise variance $\mathbf{Z}$ in the public parameters pub.

Noise Computed by (8), returning $\underline{y}'_k$ as the noisy measurement at time k, with added pseudorandom Gaussian noise computed from the stream cipher using sk.

In addition, we note that in the above Setup algorithm, the inclusion of the initial state and additional noise covariance are not a requirement for the security of the scheme, but merely makes relevant estimation parameters public for completeness.

The idea behind our security roof relies on the optimality of the linear Kalman Filter (KF) [17].

The KF produces estimates with the smallest achievable error covariance, with respect to mean square error (MSE), achievable for *any* estimator when all measurements $\underline{y}_1, \ldots, \underline{y}_k$ are observed.

Given an initial estimate and estimate error covariance, the KF recursively makes estimates

When noises are Gaussian and models linear, the KF computes an estimate

The idea behind our security proof relies on the Cramér–Rao lower bound (CRLB) [18]. The CRLB gives the smallest achievable error covariance, with respect to root mean square error (RMSE), achievable for *any* estimator when all measurements $\underline{y}_1, \ldots, \underline{y}_k$ are observed. Notably, the CRLB can be computed exactly when process and measurement models are Gaussian and linear.

The CRLB can also be computed recursively for time k, in which case it reduces to the posterior estimate error covariance at time k as given by the linear Kalman Filter []. This is given by

...recursive equations for the update covariance of the KF (predict and update combined, but predict first). (Note is this true?? Might need biased CRLB - when is it the best?? What assumptions are made??)

which gives us a value $\mathbf{P}_k$ at time k, such that

$$\mathbf{P}_k \preceq \mathsf{Cov}\left[\mathcal{A}\left(k, \mathcal{M}_P, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k\right) - \underline{x}_k\right] \tag{16}$$

for any estimator $\mathcal{A}$ following definition II.1 and any Gaussian, linear, time-invariant models $\mathcal{M}_P$ and $\mathcal{M}_M$.

This leads us into our sketch proof.

Proof sketch: (LaTeXdescription? sub(sub)section?)

As we use a cryptographically pseudorandom stream cipher, the stream integers g and generated pseudorandom uniformly distributed floating point numbers u are indistinguishable from random integers and floating-point number by any polynomially bound estimator.

Additionally, we argue that the uniformly distributed floating point numbers u are sufficiently close to real standard uniform numbers $\mathcal{U}(0,1)$ for all the necessary estimation properties and lower bounds to hold. This is the standard in

estimation tasks due to the inexistence of true real numbers on modern computer hardware.

In turn, this leads to pseudorandom noisy measurements $\underline{y}'_k$ that are indistinguishable from real measurements following the noisy measurement model () exactly.

We can now compute the CRLB recursively for both the true measurement model (), obtaining series $\{\mathbf{P}_1, \mathbf{P}_2, \dots\}$, and the modified model (), obtaining series $\{\mathbf{P}'_1, \mathbf{P}'_2, \dots\}$. Due to models' properties $R < R + Z$, and the properties of the CRLB, taking the difference of the two series for *any* initial covariance $\mathbf{P}_0$ produces the infinite series of valid covariances $\mathbf{D}_1, \mathbf{D}_2, \dots$, where

$$\mathbf{D}_k = \mathbf{P}'_k - \mathbf{P}_k \,. \tag{17}$$

Since both series $\mathbf{P}_k$ and $\mathbf{P}'_k$ give the lowest possible error covariance of respective estimators, an estimator following model () can always be created for an estimator following the modified model () such that their error covariances at any time k differs by at least $\mathbf{D}_k$.

A reduction proof can be easily constructed where the existence of an unprivileged estimator in our scheme that can produce estimates such that (4) does not hold, can be used to construct an estimator with an error covariance lower than $\mathbf{P}'_k$ given the modified model. As we know that no such estimator exists, we conclude that our scheme meets $\{\mathbf{D}_1, \mathbf{D}_2, \dots\}$-Covariance Privilege for Models $\mathcal{M}_P$ and $\mathcal{M}_M$, when $\mathcal{M}_P$ and $\mathcal{M}_M$ are Gaussian, linear and time-invariant.

End proof sketch.

In addition to the proof sketch above, we stress caution when assuming accepting a cryptographic guarantee in terms of models $\mathcal{M}_P$ and $\mathcal{M}_M$ when used to predict a measured physical process. The following implicit assumptions would be made in such a scenario.

Exact models When assigning a model to a physical process, our scheme involving the model only guarantees the same security of estimating the physical process when it follows the model *exactly*. It is often the case that models are chosen to be Gaussian and linear in part to simplify estimation, resulting in the possibility of better estimation with alternative, more complicated, models. While it may be likely that the estimation of an unprivileged estimator is worse even when this is the case, it cannot be proved by our methodology here.

Bayesian interpretation We also note that the model requirements and security definitions we have put forward assume a Bayesian interpretation of probability theory. Although this is the standard for state estimation problems due to its applicability and performance, without stating this assumption it may be arguable that the security definition 4 may not hold.

B. Multiple Additional Noises

While we have not defined a security notion for multiple levels of privileged estimation, an intuitive and informal extension can be described.

The security notion desired would require that for any subset of corrupted estimators, and therefore the knowledge of any subset of different privilege level secret keys $s \subset \{\mathsf{sk}_i, 0 \leq i < N\}$ and noisy measurements, an estimator which is given true measurements can be constructed, such that the difference between the corrupted subset's error covariance and its own is at least $\mathbf{D}_k^{(s)}$ at time k.

Although this definition requires an infinite series for every possible subset of privilege level keys s, complicating its form specification, it captures the exact advantage of every such subset making it a more general definition.

Given the structure of our scheme in section () it can be readily seen how the above notion would be met. Similarly to the single level case, the CRLB can be used to compute the minimum error covariances for all compromised key subsets as well as for an estimator with the true measurements, and the relevant infinite covariance series' can be defined.

V. Simulation and Results

As well as showing the theoretical security of our scheme, we have simulated the estimation problem using linear Kalman filter estimators which achieve the CRLB error covariances for the different measurement models. Simulations have been implemented in the Python programming language and use the AES block cipher in CTR mode as a cryptographically secure stream cipher (AES-CTR) [].

We have considered two simulations, both following the same two-dimensional constant-velocity process model, given by

$$\mathbf{F} = \begin{bmatrix} 1 & 0.5 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0.5 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and

$$\mathbf{Q} = 0.01 \cdot \begin{bmatrix} 0.0417 & 0.1250 & 0 & 0 \\ 0.1250 & 0.5000 & 0 & 0 \\ 0 & 0 & 0.0417 & 0.1250 \\ 0 & 0 & 0.1250 & 0.5000 \end{bmatrix},$$

with differing measurement models. In all cases, estimators were initialised with the same initial conditions, equal to the true starting condition of the processes they were estimating.

The first measurement model measures location and leads to an observable system with bounded CRLB error covariances as $k \to \infty$. It is given by

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ and } \mathbf{R} = \begin{bmatrix} 5 & 2 \\ 2 & 5 \end{bmatrix},$$

and the sensor adds pseudorandom Gaussian samples with covariance

$$\mathbf{Z} = \begin{bmatrix} 35 & 0 \\ 0 & 35 \end{bmatrix}$$

to create an estimator privilege level. Figures () and () show the average error covariance traces and RMSE of estimation from 1000 runs of our privileged estimation scheme, respectively, where the above models are followed. It can be seen that

the trace of the privileged estimator error covariance is lower than that of the unprivileged one. Both traces are equivalent to the those of respective estimator CRLB covariances and their difference equal to the trace of the estimation privilege covariance $\mathbf{D}_k$ at any time k.

The second simulation considers an unobservable system where only the velocity is measured and has an unbounded CRLB error covariance as $k \to \infty$. It is given by

$$\mathbf{H} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and uses the same values for $\mathbf{R}$ and $\mathbf{Z}$ as given for the previous model. Figures () and () show the average error covariance traces and RMSE of estimation from 1000 runs using this model and capture how error covariance boundedness does not affect the privileged estimation scheme's properties.

Lastly, a simulation of multiple privilege levels was also performed using the bounded error covariance measurement model () and using pseudorandom Gaussian sample with variances $\mathbf{Z}_0 = 20 \cdot \mathbf{I}$, $\mathbf{Z}_1 = 14 \cdot \mathbf{I}$ and $\mathbf{Z}_2 = 17 \cdot \mathbf{I}$. Note that the three matrices $\mathbf{Z}_i$, $0 \leq i < 3$ are such that () is satisfied. Figures () and () again show the average traces and RMSE of estimation from 1000 runs and display the distinct difference in estimation error of the different privilege levels. Additionally, two special case bounding estimators are included, one holding all privilege level keys and one holding none.

All of the included figures capture the difference in estimation error of the best possible estimators given the simulated processes (with respect to RMSE) and support the proposed security proof sketch given in section ().

VI. Conclusion

Presented the idea of privileged estimation and gave a formal cryptographic definition.

Demonstrated a concrete privileged estimation scheme and gave a proof sketch for it meeting the desired security notion.

Additionally supported the proof sketch by simulation using the best possible estimators for the simulated processes.

Future work includes reducing the requirement () for multiple levels of private estimation, discussing the formal security in this case further and implementing privileged estimation on hardware to demonstrate the real-time capability of the method.

References

[1] M. Liggins, C. Y. Chong, D. Hall, and J. Llinas, *Distributed Data Fusion for Network-Centric Operations*. CRC Press, 2012.

[2] A. G. O. Mutambara, *Decentralized Estimation and Control for Multisensor Systems*. CRC press, 1998.

[3] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, Sep. 2004.

[4] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[5] 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.

[6] S. Gueron, "Intel Advanced Encryption Standard (AES) New Instructions Set," *Intel Corporation*, 2010.

[7] 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.

[8] J. Katz and Y. Lindell, *Introduction to Modern Cryptography: Principles and Protocols*. Chapman & Hall, 2008.

[9] A. Alanwar, Y. Shoukry, S. Chakraborty, P. Martin, P. Tabuada, and M. Srivastava, "PrOLoc: Resilient Localization with Private Observers Using Partial Homomorphic Encryption," in *16th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2017, pp. 41–52.

[10] A. B. Alexandru and G. J. Pappas, "Private Weighted Sum Aggregation," *arXiv*, 2020.

[11] A. B. Alexandru, M. S. Darup, and G. J. Pappas, "Encrypted Cooperative Control Revisited," in *58th IEEE Conference on Decision and Control (CDC)*, 2019, pp. 7196–7202.

[12] F. Farokhi, I. Shames, and N. Batterham, "Secure and Private Control Using Semi-Homomorphic Encryption," *Control Engineering Practice*, vol. 67, pp. 13–20, 2017.

[13] P. D. Groves, "Principles of GNSS, inertial, and multisensor integrated navigation systems, 2nd edition [Book review]," *IEEE Aerospace and Electronic Systems Magazine*, vol. 30, no. 2, pp. 26–27, Feb. 2015.

[14] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission Scheduling for Remote State Estimation Over Packet Dropping Links in the Presence of an Eavesdropper," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3732–3739, Sep. 2019.

[15] F. Goualard, "Generating Random Floating-Point Numbers by Dividing Integers: A Case Study," *Computational Science (ICCS)*, vol. 12138, 2020.

[16] R. E. A. C. Paley and N. Wiener, *Fourier Transforms in the Complex Domain*. American Mathematical Soc., Dec. 1934.

[17] R. E. Kalman, "A New Approach to Linear Filtering and Prediction Problems," *Journal of Basic Engineering*, vol. 82, no. 1, pp. 35–45, 1960.

[18] A. J. Haug, "Bayesian Estimation and Tracking," p. 397.