AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your paper. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

Carefully check the page proofs (and coordinate with all authors); additional changes or updates WILL NOT be accepted after the article is published online/print in its final form. Please check author names and affiliations, funding, as well as the overall article for any errors prior to sending in your author proof corrections. Your article has been peer reviewed, accepted as final, and sent in to IEEE. No text changes have been made to the main part of the article as dictated by the editorial level of service for your publication.

AQ1: Please confirm or add details for any funding or financial support for the research of this article.

AQ2: Please provide the URL address for Reference [12].

AQ3: Please provide the month for Reference [14].

AQ4: Please confirm if the location and publisher information for Reference [15] is correct as set.

AQ5: Please confirm the volume number for Reference [17].

Cryptographically Privileged State Estimation With Gaussian Keystreams

Marko Ristic, Benjamin Noack, *Member, IEEE*, and Uwe D. Hanebeck, *Fellow, IEEE*

***Abstract*—State estimation via public channels requires additional planning with regards to state privacy and 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 that make this distinction typically result in reduced estimation quality, require additional communication channels, or lack a formal cryptographic backing. We introduce a method to decrease estimation quality at an unprivileged estimator using a stream of pseudorandom Gaussian samples while leaving privileged estimation unaffected and requiring no additional transmission beyond an initial key exchange. First, a cryptographic definition of privileged estimation is given, capturing the difference between privileges, before a privileged estimation scheme meeting the security notion is presented. Achieving cryptographically 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.**

***Index Terms*—Encrypted state estimation, Kalman filtering, stream ciphers.**

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 cryptographically guaranteeing data privacy over public channels involve hiding all transferred information such that eavesdroppers or untrusted parties learn no additional information from any observed data. This is achievable using common encryption schemes such as AES [6] or RSA [7], which formally capture this requirement by satisfying cryptographic ciphertext indistinguishability [8, Ch. 3]. However, 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. In control theory, [9] uses an aggregation scheme to combine distributed control inputs without learning individual contributions, while [10], [11] use homomorphic encryption to allow control inputs to be computed without decryption. In estimation, [12] proposes navigation where individual sensor information and measurements remain private, while [13] fuses encrypted estimates using only their error covariance ratios. Within the context of estimation, a quantifiable difference in estimation performance between untrusted and trusted parties can also provide levels of estimation *privilege*. This was achieved in the original Global Positioning System (GPS) [14], which relied on an additional encrypted channel for more accurate estimation. In another approach, [15], [16], additive noise is used to increase eavesdropper estimation error by using a synchronized chaotic system and at the physical layer, respectively. These methods provide a solution to the privileged estimation problem but have not had their security guarantees cryptographically proven, and in [16], an extension to multiple estimation privileges would require additional hardware. Our contribution in this work considers this context of privileged and unprivileged estimation and is comprised of a novel formal definition of privileged state estimation, crucial for cryptographic security, before proposing a scheme that provides one or more privileged levels of estimation without reliance on additional secure channels. We accompany the method with a cryptographic proof sketch and simulation results.

In Section II, we introduce the cryptographic formalization for privileged estimation followed by the relevant estimation problem. 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 explained and demonstrated in Section V, while concluding remarks and future work are discussed in Section VI.

Manuscript received March 4, 2021; revised May 7, 2021; accepted May 24, 2021. Recommended by Senior Editor J.-F. Zhang. (AQ1)
(Corresponding author: Marko Ristic.)

Marko Ristic and Uwe D. Hanebeck are with the Intelligent Sensor-Actuator-Systems Laboratory, Institute for Anthropomatics, Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany (e-mail: marko.ristic@kit.edu; uwe.hanebeck@kit.edu).

Benjamin Noack is with Autonomous Multisensor Systems Group, Institute for Intelligent Cooperating Systems, Otto von Guericke University Magdeburg, 39106 Magdeburg, Germany (e-mail: benjamin.noack@ovgu.de).
Digital Object Identifier 10.1109/LCSYS.2021.3084405

A. Notation

Lowercase underlined characters $\underline{a}$ are vectors and uppercase bold characters $\mathbf{M}$ are matrices. $\mathbf{M} \succ 0$ and $\mathbf{M} \succeq 0$ denote positive definitiveness and semi-definitiveness, respectively, and $\mathbf{M} \succ \mathbf{N}$ is short for $\mathbf{M} - \mathbf{N} \succ 0$. $\mathbf{I}$ and $\mathbf{0}$ are the identity and zero matrices, respectively, with sizes inferrable from context and the function $\mathsf{eig}(\mathbf{M})$ gives the set of eigenvalues for matrix $\mathbf{M}$. $\mathsf{Cov}[\cdot]$ computes the covariance of a random vector, $\sim$ denotes distribution, $\dot{\sim}$ denotes pseudorandom distribution, and $\mathcal{A}(\underline{i})$ denotes the output of an arbitrary algorithm $\mathcal{A}$ given inputs $\underline{i}$.

II. Problem Statement

In this work, we consider the estimation scenario where system and measurement models are known and stochastic, and state estimators are either privileged, when holding a secret key, or unprivileged, without. Our goal is to develop a scheme that quantifies and cryptographically guarantees the difference between their estimation errors when models are Gaussian and linear.

To capture the aim of creating a privileged and unprivileged estimator, we must first define how to assess estimation advantage between them, and which algorithms are required to characterize a privileged estimation scheme. In this section, we give the relevant formal definitions for security, followed by the system and measurement models considered in this work.

A. Formal Cryptographic Problem

While we later introduce assumptions on the system and measurement 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. Afterward, we will show that our proposed scheme meets this security notion under the specific Gaussian and linear 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, Ch. 3]. 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 in terms of a time series of covariances, given arbitrary known 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 formalize this, we introduce the following notations and definitions. We assume the existence of an arbitrary process (not necessarily Gaussian or linear) following a known system model exactly, with the state at time step k denoted by $\underline{x}_k \in \mathbb{R}^n$ and model parameters $\mathcal{M}_S$. Similarly, we assume the existence of a means of process measurement following a known measurement model exactly, with the measurement at time step k denoted by $\underline{y}_k \in \mathbb{R}^m$ and model parameters $\mathcal{M}_M$. We can now define a relevant scheme.

Definition 1: A *privileged estimation scheme* is a pair of probabilistic algorithms (Setup, Noise), given by

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

$\mathsf{Noise}(\mathsf{pub}, \mathsf{sk}, k, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \dots, \underline{y}_k)$: On input of public parameters pub, secret key sk, time step k, models $\mathcal{M}_S$ and $\mathcal{M}_M$, and measurements $\underline{y}_1, \dots, \underline{y}_k$, a noisy measurement $\underline{y}'_k$ (with no required model constraints) is created.

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

Definition 2: An *estimator* is any probabilistic algorithm that produces a guess of the state $\underline{x}_k$ for a given time step k.

Definition 3: A *negligible covariance function*,

$$\mathsf{neglCov}_m(\kappa) : \mathbb{N} \to \mathbb{R}^{m \times m}, \tag{1}$$

is a function 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 for each of its eigenvalues $e \in \mathsf{eig}(\mathbf{A})$, there exists a negligible function [8, Definition 3.4] η such that $e \leq \eta(\kappa)$.

We can now introduce the security notion that captures the formal requirements of the problem we want to solve.

Definition 4: A privileged estimation scheme meets notion $\{\mathbf{D}_1, \mathbf{D}_2, \dots\}$*-Covariance Privilege for Models* $\mathcal{M}_S$ *and* $\mathcal{M}_M$ if for any PPT estimator $\mathcal{A}$, there exists a PPT estimator $\mathcal{A}'$, such that

$$\begin{aligned}
&\mathsf{Cov}\Big[\mathcal{A}\Big(k, \kappa, \mathsf{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}'_1, \dots, \underline{y}'_k\Big) - \underline{x}_k\Big] \\
&\quad - \mathsf{Cov}\Big[\mathcal{A}'\Big(k, \kappa, \mathsf{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \dots, \underline{y}_k\Big) - \underline{x}_k\Big] \\
&\quad \succeq \mathbf{D}_k + \mathsf{neglCov}_m(\kappa)
\end{aligned} \tag{2}$$

for valid covariances $\mathbf{D}_k$ and some negligible covariance function 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 randomness introduced in models $\mathcal{M}_S$ 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 $\underline{y}'_1, \dots, \underline{y}'_k$ can estimate a state $\underline{x}_k$ for a time step k with a mean square error (MSE) covariance less than an equivalent estimator with access to true measurements $\underline{y}_1, \dots, \underline{y}_k$, by a margin of at least $\mathbf{D}_k$. We also note that by taking probabilities over randomness introduced in the system model, and therefore the possible true states $\underline{x}_k$, the definition fits a Bayesian interpretation of probability for any stochastic system model.

B. Estimation Problem

With the relevant security definitions above, we now give the specific estimation models required for our scheme. The system model we consider gives the state $\underline{x}_k \in \mathbb{R}^n$ at an integer time step k and is given by

$$\underline{x}_k = \mathbf{F}_k \underline{x}_{k-1} + \underline{w}_k, \tag{3}$$

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

$$\underline{y}_k = \mathbf{H}_k \underline{x}_k + \underline{v}_k, \tag{4}$$

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

Next, we propose a privileged estimation scheme meeting definition 4 for a derivable series of covariances when models $\mathcal{M}_S$ and $\mathcal{M}_M$ are of the form (3) and (4), respectively.

III. Privileged Estimation

The key idea behind the privileged estimation scheme we propose is to add pseudorandom noise to existing measurement noise 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 removed from measurements by any estimator holding the same key.

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

A. Gaussian Keystream

To generate pseudorandom Gaussian samples, we choose to rely on first generating a typical cryptographic pseudorandom bitstream given a secret key sk. This can be done with any cryptographic stream cipher and will reduce the security of our scheme to a single, well-studied, and replaceable component. We interpret the bitstream as sequential pseudorandom integers $q_t \in \mathbb{N}$, of a suitable size, for integer indices $t > 0$ 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 is complicated. For now, we will assume that the uniform floating-point numbers (floats) 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, [17]. In Section IV, we will state and further discuss this assumption.

Given the sufficiently uniform pseudorandom floats 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 [18], by

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

and

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

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

B. Additional Gaussian Noise

To use the series of pseudorandom Gaussian samples z_t, $t > 0$, 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 (4), at every time step k. As we want control over the difference in estimation error between privileged and unprivileged estimators, we do so by including the symmetric matrix parameter $\mathbf{Z} \succ 0$, in a way that added pseudorandom noise $\underline{p}_k$ at time step 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 $(k-1)n + 1 \le t \le kn$, as

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

for any matrix $\mathbf{A}$ such that $\mathbf{A}\mathbf{A}^\top = \mathbf{Z}$. We also note that for the correct removal of noise terms $\underline{p}_k$ by the privileged estimator, index information k is required when communication channels are lossy or have some delay. While estimation over the Internet may use the indexing information already present in TCP/IP, for the remainder of the work we consider the case when all measurements arrive, in order, and neglect additional index information for the sake of simplicity.

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 measurements $\underline{y}_k$ by

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

resulting in a new measurement model

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

with $\underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k)$ 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, $t > 0$, and therefore the added noise vectors $\underline{p}_k$ at every time step k. Computing $\underline{y}_k = \underline{y}'_k - \underline{p}_k$ given the noisy measurements results in the original measurements following measurement model (4) 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 unprivileged measurement model

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

with $\underline{v}'_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k + \mathbf{Z})$, 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 $\mathbf{D}_k$, $k > 0$, required for the security notion in definition 4.

C. Multiple Privileges

In the above scenario, we have considered a single estimation privilege 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

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

with $\underline{p}_k^{(i)} \stackrel{c}{\sim} \mathcal{N}(\underline{0}, \mathbf{Z}_i)$, $1 \leq i \leq N$. 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 $\mathbf{Z}_i$, is removed, resulting in measurements indistinguishable from those following the unprivileged measurement model

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

where $\underline{v}_k^{(i)} \sim \mathcal{N}(\underline{0}, \mathbf{R}_k + \mathbf{E}_i)$, 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 $\mathbf{R}_k$, it is clear that $\mathbf{E}_i \succ 0$ and $\mathbf{E}_i = \mathbf{E}_i^\top$ 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 level privileged estimation case as introduced in Section III-B and a proof sketch will be provided to show how the proposed scheme meets the cryptographic notion in definition 4. The extension to multiple privilege levels as described in Section III-C will be informally discussed afterward.

A. Single Privileged Case

Recalling definition 4, we aim to show how the notion is met by our single privilege level estimation scheme. Before the proof sketch, we look at our scheme in the context of a formal privileged estimation scheme with model constraints and give some relevant optimality properties.

We consider the stochastic system model (3) and measurement model (4) exactly, that is, any linear models with known covariance, zero-mean, Gaussian additive noises. We define these as our model conditions and capture all relevant parameters from the respective equations in $\mathcal{M}_S$ and $\mathcal{M}_M$. Our scheme fulfills the two required algorithms for a privileged estimation scheme, Setup and Noise, as follows.

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

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

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

The idea behind our security proof relies on the optimality of the linear Kalman Filter (KF) [19]. Given an initial estimate and its error covariance, the KF produces posterior estimates with the minimum mean square error (MSE) achievable for *any* estimator when all measurements $\underline{y}_1, \ldots, \underline{y}_k$ are observed, models are Gaussian and linear, and the same initialization is used. Since the KF also preserves initial error covariance order,

$$\mathbf{P}_k \preceq \mathbf{P}_k' \implies \mathbf{P}_{k+1} \preceq \mathbf{P}_{k+1}', \tag{16}$$

we can define an error covariance lower-bound $\mathbf{P}_k^{(l)}$ for all possible initialisations by setting $\mathbf{P}_0^{(l)} = \mathbf{0}$ and computing the posterior KF error covariance using the combined predict and update equations

$$\begin{aligned} \mathbf{P}_k^{(l)} = &\Big(\mathbf{I} - (\mathbf{F}_k \mathbf{P}_{k-1}^{(l)} \mathbf{F}_k^\top + \mathbf{Q}_k)\mathbf{H}_k^\top \\ &\cdot \Big(\mathbf{H}_k (\mathbf{F}_k \mathbf{P}_{k-1}^{(l)} \mathbf{F}_k^\top + \mathbf{Q}_k)\mathbf{H}_k^\top + \mathbf{R}_k\Big)^{-1} \mathbf{H}_k\Big) \\ &\cdot \Big(\mathbf{F}_k \mathbf{P}_{k-1}^{(l)} \mathbf{F}_k^\top + \mathbf{Q}_k\Big). \end{aligned} \tag{17}$$

This gives us a lower-bound at every time step k, such that

$$\mathbf{P}_k^{(l)} \preceq \mathsf{Cov}\Big[\mathcal{A}\Big(k, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \ldots, \underline{y}_k\Big) - \underline{x}_k\Big] \tag{18}$$

for any estimator $\mathcal{A}$ following definition 2 and any Gaussian and linear models $\mathcal{M}_S$ and $\mathcal{M}_M$. This leads us to the security proof sketch.

Theorem 1: Our single privilege estimation scheme in Section III-B meets $\{\mathbf{D}_1, \mathbf{D}_2, \ldots\}$-Covariance Privilege for Models $\mathcal{M}_S$ and $\mathcal{M}_M$, for a computable series $\mathbf{D}_k$, $k > 0$ dependent on a noise parameter $\mathbf{Z}$, when $\mathcal{M}_S$ and $\mathcal{M}_M$ are Gaussian and linear.

Proof Sketch: Since a cryptographically pseudorandom stream cipher is used in Section III-A, the stream integers q_t, and therefore the uniform samples u_t and normal Gaussian samples z_t, are indistinguishable to those generated from a truly random stream for any PPT estimator without the secret key. We persist with the previous assumption that floating-point representations of z_t are sufficiently close to Gaussian and assume the KF to provide optimal estimation when using floats, as is standard in the state-of-the-art. Using the Setup and Noise algorithms for our scheme now leads to pseudorandom noisy measurements $\underline{y}'_k$ that are indistinguishable from measurements following the unprivileged measurement model (10). We can now compute a lower-bound $\mathbf{P}'^{(l)}_k$ for any unprivileged estimator as $\mathbf{P}'^{(l)}_0 = \mathbf{0}$ and

$$\begin{aligned}\mathbf{P}'^{(l)}_k = \Big(&\mathbf{I} - (\mathbf{F}_k\mathbf{P}'^{(l)}_{k-1}\mathbf{F}_k^\top + \mathbf{Q}_k)\mathbf{H}_k^\top \\ &\cdot\Big(\mathbf{H}_k(\mathbf{F}_k\mathbf{P}'^{(l)}_{k-1}\mathbf{F}_k^\top + \mathbf{Q}_k)\mathbf{H}_k^\top + \mathbf{R}_k + \mathbf{Z}\Big)^{-1}\mathbf{H}_k\Big) \\ &\cdot\Big(\mathbf{F}_k\mathbf{P}'^{(l)}_{k-1}\mathbf{F}_k^\top + \mathbf{Q}_k\Big). \end{aligned} \tag{19}$$

Taking the difference of (19) and (17) produces the series

$$\mathbf{D}_k = \mathbf{P}'^{(l)}_k - \mathbf{P}^{(l)}_k, \tag{20}$$

for $k > 0$, which can be tuned by the parameter $\mathbf{Z}$. Since both series $\mathbf{P}^{(l)}_k$ and $\mathbf{P}'^{(l)}_k$ give the lowest possible error covariance of the respective estimators, an estimator knowing model (4) can always be created for one knowing only model (10) such that their error covariances at any time step k differ 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 (2) does not hold, can be used to construct an estimator with an error covariance lower than $\mathbf{P}'^{(l)}_k$ given a known model of the form (10). As no such estimator exists, we conclude that our scheme meets $\{\mathbf{D}_1, \mathbf{D}_2, \ldots\}$-Covariance Privilege for Models $\mathcal{M}_S$ and $\mathcal{M}_M$, when $\mathcal{M}_S$ and $\mathcal{M}_M$ are Gaussian and linear. This concludes our proof sketch.

In addition to the proof sketch, we stress caution when accepting a cryptographic guarantee in terms of models $\mathcal{M}_S$ and $\mathcal{M}_M$ when used to estimate a measured physical process or approximate continuous quantities. The following assumptions are made in this scenario.

Exact Models: When assigning a model to a physical process, any cryptographic guarantees concerning the model assume the process follows the model *exactly*. It is often the case that models assume a Bayesian interpretation of probability (a stochastic state) or are chosen to simplify estimation, resulting in the possibility of better estimation given alternative or more complicated models. Although the standard for state estimation, we state the assumption to highlight the distinction between models and a physical process.

Floating-Point Approximation: As stated in Section III-A and the proof sketch above, floating-point approximations to real numbers complicate cryptographic guarantees when relying on proofs using real numbers such as KF optimality. While optimal estimation with floats is beyond the scope of this work, the prevalence of floats in decades of state estimation justifies the assumption of sufficient similarity and the insignificance of associated error introduced to the security notion.

B. Multiple Additional Noises

We have not defined a security notion for multiple levels of privileged estimation from Section III-C, but an intuitive and informal extension is briefly described here.

A suitable notion would require that for any subset of corrupted estimators, and thus estimators with any subset of secret keys $S \subseteq \{\mathsf{sk}_i,\ 1 \leq i \leq N\}$, who are given noisy measurements $\underline{y}''_k$, an estimator given true measurements $\underline{y}_k$ can be constructed such that the difference between the corrupted subset's error covariance and its own is at least $\mathbf{D}^{(S)}_k$ at time step k. Although this definition requires a series $\mathbf{D}^{(S)}_k$ for every possible subset of keys, S, complicating its formal specification, it captures the exact advantage of every such subset producing a general definition.

Given the structure of our scheme in Section III-C, it can be readily seen how the above notion would be met. Similarly to the single level case, the KF 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 difference series $\mathbf{D}^{(S)}_k$ can be defined.

V. Simulation and Results

As well as showing the theoretical security of our scheme, we have simulated the stochastic estimation problem using linear Kalman filter estimators for the different measurement models. Simulations have been implemented in the Python language and use the AES block cipher in CTR mode as a cryptographically secure stream cipher (AES-CTR) [6].

We consider two simulations, both following the same two-dimensional time-invariant constant velocity system model, given by

$$\mathbf{F}_k = \begin{bmatrix} 1 & 0.5 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0.5 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \mathbf{Q}_k = \frac{1}{10^3} \cdot \begin{bmatrix} 0.4 & 1.3 & 0 & 0 \\ 1.3 & 5.0 & 0 & 0 \\ 0 & 0 & 0.4 & 1.3 \\ 0 & 0 & 1.3 & 5.0 \end{bmatrix},$$

for all k, with differing measurement models. In all cases, estimators were initialized with the same initial conditions, equal to the true starting condition of the system they were estimating, with initial error covariance $\mathbf{0}$.

The first measurement model measures location and leads to an observable system with bounded error covariances as $k \to \infty$. It is given by $\mathbf{H}_k = \left[\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right]$ and $\mathbf{R}_k = \left[\begin{smallmatrix} 5 & 2 \\ 2 & 5 \end{smallmatrix}\right]$, for all k, and the sensor adds pseudorandom Gaussian samples with covariance $\mathbf{Z} = 35 \cdot \mathbf{I}$ to create an estimator privilege level. Figure 1 shows the average error covariance traces and the mean square error (MSE) of estimation from 1000 runs of

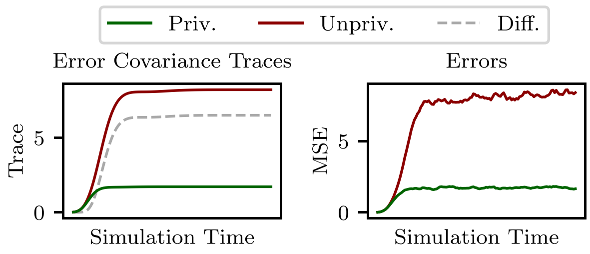

Fig. 1. Privileged estimation with bounded error covariance.

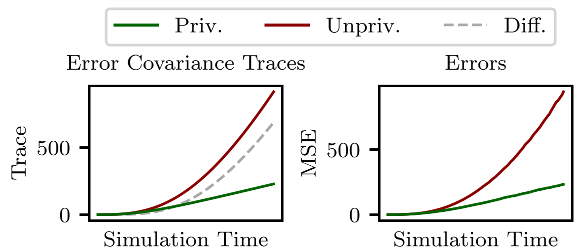

Fig. 2. Privileged estimation with unbounded error covariance.

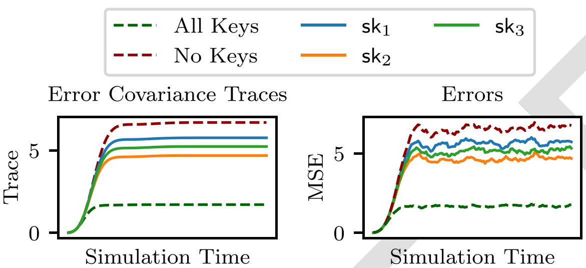

Fig. 3. Estimation with multiple privilege levels.

our privileged estimation scheme, where the above models are followed. It can be seen that the trace of the privileged estimator's error covariance stays lower than that of the unprivileged one and that privileged estimation has lower MSE. The difference in trace between the two estimators has also been plotted and is equal to the trace of the series (20) for all time steps k due to the chosen initial error covariance.

The second simulation considers an unobservable system where only the velocity is measured and has an unbounded error covariance as $k \to \infty$. It is given by $\mathbf{H}_k = \left[\begin{smallmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$, for all k, and uses the same values for $\mathbf{R}_k$ and $\mathbf{Z}$ as the previous model. Figure 2 shows the average error covariance traces and MSE of estimation from 1000 runs using this model and captures 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 samples such that $\mathbf{E}_1 = 20 \cdot \mathbf{I}$, $\mathbf{E}_2 = 14 \cdot \mathbf{I}$, and $\mathbf{E}_3 = 17 \cdot \mathbf{I}$ for estimators holding the single keys sk_1, sk_2 and sk_3, respectively. Note that the three matrices $\mathbf{E}_i$, $1 \leq i \leq 3$ satisfy (15). Figure 3 again shows the average traces and MSE of estimation from 1000 runs and displays the distinct difference in estimation error of the different privilege levels. Additionally, two special cases that bound all estimators are included, one holding all privilege level keys and another holding none.

All of the included figures capture the difference in estimation error between the best possible estimators given the simulated processes (in terms of MSE) and support the proposed security proof sketch given in Section IV.

VI. Conclusion

In this work, we have presented the idea of a privileged estimation scheme and given a formal cryptographic definition for its security. A concrete scheme was provided that meets this notion and an intuitive extension to multiple privilege levels was discussed. A simulation demonstrating a simple use case has been presented, while the benefits of controlling estimation accuracy on a per-party basis have wide application from privatized localization hardware to subscription-based data access. Future work on the topic includes achieving formal security for broader model requirements and testing our scheme on dedicated hardware to demonstrate the method's real-time capability.

References

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

[2] A. G. O. Mutambara, *Decentralized Estimation and Control for Multisensor Systems*. Hoboken, NJ, USA: 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 Trans. Autom. 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 Comput.*, vol. 16, no. 1, pp. 69–73, Jan./Feb. 2012.

[5] M. Brenner, J. Wiebelitz, G. von Voigt, and M. Smith, "Secret program execution in the cloud applying homomorphic encryption," in *Proc. 5th IEEE Int. Conf. Digit. Ecosyst. Technol. (DEST)*, 2011, pp. 114–119.

[6] S. Gueron, *Intel Advanced Encryption Standard (AES) New Instructions Set*, Intel, San Jose, CA, USA, 2010.

[7] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

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

[9] A. B. Alexandru and G. J. Pappas, "Private weighted sum aggregation," 2020. [Online]. Available: arxiv.org/abs/2010.10640

[10] A. B. Alexandru, M. S. Darup, and G. J. Pappas, "Encrypted cooperative control revisited," in *Proc. 58th IEEE Conf. Decis. Control (CDC)*, 2019, pp. 7196–7202.

[11] F. Farokhi, I. Shames, and N. Batterham, "Secure and private control using semi-homomorphic encryption," *Control Eng. Pract.*, vol. 67, pp. 13–20, Oct. 2017.

[12] M. Ristic, B. Noack, and U. D. Hanebeck, "Privacy-preserving localization using private linear-combination aggregation," *IEEE Trans. Autom. Control*, early access. AQ2

[13] M. Ristic, B. Noack, and U. D. Hanebeck, "Secure fast covariance intersection using partially homomorphic and order revealing encryption schemes," *IEEE Control Syst. Lett.*, vol. 5, no. 1, pp. 217–222, Jan. 2021.

[14] P. D. Groves, "Principles of GNSS, inertial, and multisensor integrated navigation systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 30, no. 2, pp. 26–27, 2015. AQ3

[15] C. Murguia, I. Shames, F. Farokhi, and D. Nešić, "Information-theoretic privacy through chaos synchronization and optimal additive noise," in *Privacy in Dynamical Systems*. Heidelberg, Germany: Springer, 2020, pp. 103–129. AQ4

[16] A. S. Leong, A. Redder, D. E. Quevedo, and S. Dey, "On the use of artificial noise for secure state estimation in the presence of eavesdroppers," in *Proc. Eur. Control Conf. (ECC)*, 2018, pp. 325–330.

[17] F. Goualard, "Generating random floating-point numbers by dividing integers: A case study," in *Proc. Int. Conf. Comput. Sci. (ICCS)*, vol. 12138, 2020, pp. 15–28. AQ5

[18] R. E. A. C. Paley and N. Wiener, *Fourier Transforms in the Complex Domain*, vol. 19. New York, NY, USA: Amer. Math. Soc., 1934.

[19] A. J. Haug, *Bayesian Estimation and Tracking: A Practical Guide*. Hoboken, NJ, USA: Wiley, 2012.