Cryptographically Privileged State Estimation With Gaussian Keystreams

Michael Shell
School of Electrical and
Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
Email: http://www.michaelshell.org/contact.html

Homer Simpson
Twentieth Century Fox
Springfield, USA
Email: homer@thesimpsons.com

James Kirk
and Montgomery Scott
Starfleet Academy
San Francisco, California 96678–2391
Telephone: (800) 555–1212
Fax: (888) 555–1212

***Abstract*—The abstract goes here.**

I. Introduction

State estimation

Wireless and distributed estimation

Security concerns

Traditional methods hide all information, other use-cases exist

Information may be divided into privilege levels authenticating different audiences to different amounts of information [gps, anonymisation]

Our contribution in this work is comprised of a formal definition of privileged state estimation, which allows the quantification of estimation error covariance differences between privileged and unprivileged estimators, before proposing a solution to the problem accompanied by a cryptographic sketch proof and simulation results.

Section summary

A. Notation

Define vectors, matrices, encryption, pseudorandom samples, positive-definitiveness and $\prec$ for matrices, negligible function

II. Problem Statement

The estimation scenario that we consider is for known process and measurement models, where 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 timestep k and is given by

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

with noise term $\underline{w} \sim \mathcal{N}(\underline{0}, \mathbf{Q})$ 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

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

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

To capture our aim of creating a "better" and "worse" estimator, we need to define how to assess estimator privilege and what algorithms are required to provide a privileged estimation scheme. In the following section, we give relevant formal definitions, which are later referred to when assessing the security of our proposed scheme.

III. Formal cryptographic Problem

While we are interested in Gaussian, linear and time-invariant models, it is of more use to define a broader security notion that can be satisfied given specified conditions on the models. This will allow the use of the same notion in future literature and is more closely in-line with cryptography practice. Later, we will show our proposed scheme meets this broad security notion under the Gaussian, linear and time-invariant model assumptions.

Typical formal cryptographic security notions capture desired privacy properties as well as attacker capabilities [1]. The most commonly desired privacy property, cryptographic indistinguishability, is not suitable for our estimation scenario due to our desire for unprivileged estimators to still gain some information from measurements. Instead, we will require a time series of estimation error covariance differences, given arbitrary known Bayesian models, such that the difference in estimation error between estimators with and without the secret key is lower-bounded at all times by the series.

To formalise this, we introduce the following notations and definitions. We assume the existence of an arbitrary process following a known model exactly, with the state at time k denoted $\underline{x}_k \in \mathbb{R}^n$, as in section II, 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 as $\underline{y}_k \in \mathbb{R}^m$, 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 $\mathcal{M}_P$, $\mathcal{M}_M$ 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 $\mathcal{M}_P$, $\mathcal{M}_M$ and measaurements $y_1, \ldots, y_k$, a noisey 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 III.1. An *estimator* is any algorithm which produces a guess of the state $\underline{x}_k$ for a given time k.

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

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

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 $e \in \operatorname{eig}(\mathbf{A})$, 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 we want to solve.

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

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

for valid covariances $\mathbf{D}_1, \ldots, \mathbf{D}_k$ 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 with access to only noisy measurements $\underline{y}'_1, \ldots, \underline{y}'_k$ can estimate a state $\underline{x}_k$ at time k with an RMSE covariance less than an equivalent estimator with normal 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 given Gaussian, linear, and time-invariant models $\mathcal{M}_P$ and $\mathcal{M}$.

IV. Privileged Estimation

General idea

(picture ?)

Use a cryptographically secure key stream to generate pseudorandom Gaussian samples

Samples are used to increase the uncertainty of estimation and are known and removable only by those with the key used to generate them

A. Gaussian Keystream

To generate pseudorandom Gaussian samples, we rely on first generating a traditional pseudorandom bitstream given a secret key.

Using well-studied methods for the generation of pseudorandomness guarantees robustness and an easy means of updating only the relevant component when the methods used are no longer considered safe.

Any implementation of a cryptographic stream cipher can be used for our purpose and will produce a stream of bits typically combined with plaintexts to provide secure encryption.

Rather than encrypting plaintext, we interpret the bitstream as sequential pseudorandom integers g and use these to generate pseudorandom uniform real numbers in the range (0,1). u

While the uniform real samples are only approximated by floating-point numbers in the conversion from integers, we argue this is sufficiently random and discuss this further in the Security section.

Finally, independent standard Gaussian samples can then be generated from the uniform real numbers using the Box-Muller transform, and are ready to be used by our sensor and privileged filter. z

B. Additional Gaussian Noise

To use the pseudorandom Gaussian samples at the sensor and privileged estimator, they need to be converted to multivariate Gaussian samples suitable for use in the measurement model and need a means of controlling how much uncertainty is added to the unprivileged estimators.

We define the additional noise term $Z > 0$ and can transform the Gaussian samples z into pseudorandom samples o of a multivariate zero-mean Gaussian distribution with covariance Z.

Before estimation, we assume that a secret key is shared between the sensor and the privileged estimator.

During estimation, the sensor modifies its measurements at each timestep.

There are now two estimation problems present for the privileged and unprivileged estimators respectively.

For the privileged estimator who holds the shared secret key, values z, and therefore o, can be computed at any time k and received measurements modified to their original form. This in turn results in exactly the measurement model from the problem formulation.

In the case where pseudorandomness is indistinguishable from randomness, as is the case at an unprivileged estimator when using cryptographically secure Gaussian keystreams and the secret key is not known, the measurement model noise covariance can now be written as $R + Z$.

Intuitively, we can already see that the two estimators will have an estimation error covariance differing by some value dependent on Z at each time k. In the security section, we will show that the best possible error covariances achievable by the privileged and unprivileged estimators can be computed exactly by computing the Cramér–Rao lower-bound for both measurement models and that the difference between them will give an exact lower-bound on the difference between the two estimator error covariances.

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; privileged and unprivileged estimators.

As a direct extension, it may be desirable to define multiple levels of privilege, such that the best estimation performance would depend on the privilege level of the estimator.

Here we will discuss the case of multiple privilege levels where a single secret key corresponds to each level, and where noise is added in the same manner as above, for each key individually.

N noise terms are added to the original measurement equation, with variances Z_i, $0 \leq i < N$.

From the equation, we can see that obtaining any single key sk_i would lead to a measurement model with where only a single pseudorandom Gaussian noise sample, of variance Z_i, is removed.

This restricts possible estimation error bounds of each privilege level due to the dependence of measurement noise at an estimator with key sk_i, on the remaining noise terms $Z_j, j \neq i$.

If we write the covariances of added measurement model noise for holder of each key sk_i as E_i, we can capture this dependance as $E_i = \sum_{j=0,j\neq i}^{N-1} Z_j$ where both $E_i > 0$ and $Z_i > 0$.

Since choosing values E_i directly controls the estimation error differences between privileged levels, we are interested in the numerical restrictions on $E_i > 0$ which will produce valid covariances $Z_j > 0$, that can be used when adding noise at the sensor.

The dependencies between the covariances can be captured by the block matrix equation.

...equation and also block matrix inequality (might need some defining as it uses $\prec$)

Since we require $Z_i > 0$ for all $0 \leq i < N$, the restriction on the choices of privilege level additional noises E_i can be rewritten as

$$E_i \prec \frac{1}{N-2} \sum_{i=0}^{N-1} E_i \tag{5}$$

for all $0 \leq i < N$.

Alternative methods involving multiple or overlapping keys among privilege levels may allow choices of E_i to be less restricted than in the equation above. We have chosen the case with a single shared key per privilege level due to its simplicity and ability to change privilege estimation performance without needing additional key redistribution, and leave variants with fewer restrictions than () as future work.

V. Scheme Security

The security of the proposed scheme will be primarily considered in the single privileged estimation level as introduced in section ().

A proof sketch will be provided to show how the proposed scheme meets the cryptographic notion in section ().

The extension to multiple privilege levels as described in the section () will be informally discussed afterwards.

A. Single Privileged Case

Recalling the introduced security notion in section (2), we aim to show how our introduce privileged esitmation scheme, given conditions on $\mathcal{M}_P$ and $\mathcal{M}_M$, meets the desired security for a computable series $\mathbf{D}_1, \ldots, \mathbf{D}_k$ dependent on the additional noise variable Z.

We consider the process model (1) and measurement model (2) exactly, that is, any linear models with known zero-mean Gaussian additive noises. This information is captured in $\mathcal{M}_P$ and $\mathcal{M}_M$ and defines our conditions on the models.

The two required algorithms for the privileged estimation scheme, Setup and Noise, are defined such that Setup initialises the stream cipher with security parameter κ, sets the secret key sk to that of the cipher and includes initial filter estimate $\hat{\underline{x}}_0$, error covariance $\mathbf{P}_0$ and additional noise variance $\mathbf{Z}$ in the public parameters pub.

Here we note that including the initial state, error covariance and added noise variance is not a requirement for the security of our scheme, but rather just a means of making relevant estimation parameters public for completeness.

The Noise function is then given by () where $\underline{y}'_k$ is the measurement after adding a pseudorandom Gaussian sample using the stream cipher at time k.

The idea behind the proof relies on the Cramér–Rao lower bound (CRLB). The CRLB gives the smallest 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 linear and Gaussian.

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

$$\mathbf{P}_k \preceq \mathrm{Cov}\left[\mathcal{A}\left(\mathrm{k}, \mathcal{M}_\mathrm{P}, \mathcal{M}_\mathrm{M}, \underline{\mathrm{y}}_1, \ldots, \underline{\mathrm{y}}_\mathrm{k}\right) - \underline{\mathrm{x}}_\mathrm{k}\right] \tag{6}$$

for any estimator $\mathcal{A}$ following definition III.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

$$\mathbf{D}_k = \mathbf{P}'_k - \mathbf{P}_k \,. \tag{7}$$

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.

–

In addition to the security definitions and proof above, we stress caution when assuming such guarantees in the presence of a measured physical process. The following implicit assumptions are made when applying models $\mathcal{M}_P$ and $\mathcal{M}_M$ to an observable phenomenon.

the Bayesian interpretation of probability

the assumption is that model is exactly correct

an assumption that uniform floating points are uniform enough (here or in negligible difference discussion above?)

B. Multiple Additional Noises

VI. Simulation and Results

VII. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

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