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

Temporary token reference [1]. Start:

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 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 $\mathbf{R} \in \mathbb{R}^{m\times m}$.

Given the models (1) and (2), the optimal estimator with respect to mean squared error is given by the linear Kalman filter []. Estimates are computed recursively, following the combined state prediction and update equations

$$\hat{\underline{x}}_k = \dots \tag{3}$$

Optimality in terms of estimation error covariance has been proved by the Cramér–Rao lower bound (CRLB) []

(CRLB details - unbiased/biased/when is it the best/what assumptions)

III. 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 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 uniform 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 multi-variate 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.

The CRLB can be computed exactly as with the original models.

In the case where pseudorandomness is indistinguishable from randomness, as is the case at an unprivileged estimator when using cryptographically sound Gaussian keystreams and no key is shared, the measurement model can now be written as $R + Z$.

This leads to a new CRLB for the unprivileged estimator now given by different equation.

C. Multiple Privileges

In the above scenario, we have considered a single privileged estimator and one shared key with the sensor, dividing estimation uncertainly lower bounds into two groups, the privileged and the unprivileged estimators.

As an intuitive extension, it may be desirable to define multiple levels of privilege, such that the best estimation performance would depend on the key or keys available to the estimator.

In this work we consider the case where a single shared key exists for each privilege level, and that the sensor adds a noise term in the same way as in the additional noise section with each key individually.

N noise terms are added to the original measurement equation, with variances Z_i

From the equation, we can see that obtaining any single key i would lead to a measurement model with added non-removable pseudorandom Gaussian noise with variance Z_j.

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

If we write the desired measurement model noise variances at each privileged estimator i as E_i, we can cature this dependance as $E_i = \sum_{j=0, j\neq i}^{N} Z_j$ where both $E_i > 0$ and $Z_i > 0$.

Since choosing values E_i directly controls the estimation error bound computed using the CRLB, 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 $\prec$)

From the equation, we can see that the only restriction on arbitrary choices of additional noise variances E_i at each privilege level, can be chosen as long as the condition is met.

We have chosen the case with a single shared key per privilege level due to its simplicity and the ability to change privilege estimation error bounds without the need for key redistribution.

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 and have been left as future work the topic.

IV. Scheme Security

The security of the proposed scheme will be primarily considered in the single privileged and unprivileged estimator case.

A sketch of cryptographic privilege will be provided a proof sketch will be provided to show the cryptographic guarantees of the scheme.

The extension to multiple privilege levels as described in the section above will be informally reduced to the same proof sketch afterwards.

A. Single Additional Noise

Typical cryptographic security is captured by a cryptographic game which captures desired privacy properties as well as attacker capabilities [].

The most commonly desired privacy property, cryptographic indistinguishability, is not suitable for our estimation scenario due to the desire for unprivileged estimators to gain information from measurements, albeit "less" than privileged ones.

Instead, we provide a time series of known error lower-bounds for estimating the plaintext, in the context of known Bayesian process and measurement models, such that no attacker can estimate the plaintext with more accuracy than this bound.

We first assume the existence of a process following a known model exactly, with model parameters $\mathcal{M}_P$ and the state at time k denoted as $\underline{x}_k \in \mathbb{R}^n$. Similarly, we assume the existence of a means of process measurement following a known measurement model exactly, with model parameters $\mathcal{M}_M$ and the measurement at time k denoted as $\underline{y}_k \in \mathbb{R}^m$.

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 and the security parameter κ, public parameters pub and a secret key sk are created.

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

To help define the security notion we want to achieve, we first introduce the following definitions.

Estimator Any algorithm which produces a guess of the state $\underline{x}_k$ for a given time k.

Negligible Covariance Function A function

$$\mathsf{neglCov}_m(\kappa) : \mathbb{N} \to \mathbb{R}^{m \times m} \tag{4}$$

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 $e \leq \eta(\kappa)$.

The security notion we want to achieve is introduced with the above definitions as follows.

Definition IV.1. A privileged estimation scheme meets $\{\mathbf{D}_1, \mathbf{D}_2, \dots\}$*-Estimator 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

$$\begin{aligned} &\mathrm{Cov}\left[\mathcal{A}\left(\mathrm{k}, \kappa, \mathsf{pub}, \mathcal{M}_\mathrm{P}, \mathcal{M}_\mathrm{M}, \underline{\mathrm{y}}'_1, \dots, \underline{\mathrm{y}}'_\mathrm{k}\right) - \underline{\mathrm{x}}_\mathrm{k}\right] \\ &- \mathrm{Cov}\left[\mathcal{A}'\left(\mathrm{k}, \kappa, \mathsf{pub}, \mathcal{M}_\mathrm{P}, \mathcal{M}_\mathrm{M}, \underline{\mathrm{y}}_1, \dots, \underline{\mathrm{y}}_\mathrm{k}\right) - \underline{\mathrm{x}}_\mathrm{k}\right] \\ &\succeq \mathbf{D}_k + \mathsf{neglCov}_m(\kappa) \end{aligned} \tag{5}$$

for valid covariances $\mathbf{D}_1, \dots, \mathbf{D}_k$ 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 noisey measurements $\underline{y}'_1, \dots, \underline{y}'_k$ can estimate a state $\underline{x}_k$ with an RMSE covariance less than an equivalent estimator with normal measurements $\underline{y}_1, \dots, \underline{y}_k$, by a margin of at least $\mathbf{D}_k$.

–

With the security notion we aim for defined formally above, we can now provide a proof sketch, with conditions on $\mathcal{M}_P$ and $\mathcal{M}_M$, and a covariance series $\mathbf{D}_1, \dots, \mathbf{D}_k$, for which our privileged estimation scheme meets the defined security notion.

Our proposed method in the sections previously can be seen as an implementation of a privileged estimation scheme as defined above, where parameter κ is the security parameter for the required stream cipher and the secret key sk is the same as the stream cipher key, while $/mathsfpub$ contains the covariance of the added pseudorandom Gaussian noise and an initial estimate and covariance. The noise algorithm corresponds to ().

Proof sketch: We consider the process model () and measurement model () exactly, that is, any linear models with known zero-mean Gaussian additive noises.

The idea behind the proof relies on the fact that the CRLB gives the smallest RMSE covariance achievable for *any* estimator, when all measurements $\underline{y}_1, \dots, \underline{y}_k$ are observed and can be computed exactly when process and measurement models are linear and Gaussian.

The CRLB at time k can, denoted $\mathbf{J}_k^{-1}$ satisfies

$$\mathbf{J}_k^{-1} \preceq \mathrm{Cov}\left[\mathcal{A}\left(\mathrm{k}, \mathcal{M}_\mathrm{P}, \mathcal{M}_\mathrm{M}, \underline{\mathrm{y}}_1, \dots, \underline{\mathrm{y}}_\mathrm{k}\right) - \underline{\mathrm{x}}_\mathrm{k}\right] \tag{6}$$

for any estimator $\mathcal{A}$

As we use a cryptographically pseudorandom keystream, noisy measurements $\underline{y}'_k$ are indistinguishable from measurements following the modified measurement model () exactly.

Similarly, the generation of uniform ...

We can compute the CRLB recursively for both the true measurement model () and the modified model (), and take their differences to get the infinite covariance series $\mathbf{D}_1, \mathbf{D}_2, \dots$.

As we know from the CRLB proof, any estimators with the two models () and () will at least differ by $\mathbf{D}_k$ at time k.

A reduction proof can be easily constructed where an unprivileged estimator in our scheme, which produces estimates such that (neglcov eq) does not hold, can be used to construct an estimator with an error covariance lower than that of the CRLB given the modified model, known to be impossible.

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*

V. Simulation and Results

VI. 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.