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]

Contribution...

Section summary

A. Notation

Define vectors, matrices, encryption, pseudorandom samples, positive-definitness and $\prec$ for matrices

II. Problem Statement

Linear time-invariant system

Kalman filter equations

KF meets the theoretical best estimator in terms of mean square error as evident from the CRLB [estimation book]

The aim is to produce measurements such that estimators have different estimation lower bounds depending on their knowledge of a shared secret key with the sensor. This is in accordance with the Kirchoff principle [crypto book] and reduces all secrecy to a single, replaceable, uniformly random integer.

We will refer to the estimator holding a shared key with the sensor as a privileged estimator, and the one without, an unprivileged estimator.

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 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.

Prior to 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 recieved measurements modified to their original form. This inturn 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 been 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 lowerbounds into two groups, the privileged and the unprivileged estimators.

In an intuitive extension, it may be desriable 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 measureent 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 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 $E_i = \sum_{j=0,j\neq i}^{N} Z_j$.

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 which will produce valid covariances $Z_j > 0$ that can be used when adding noise at the sensor.

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

any e's achievable as long as condition met

also say it's simple Alternative methods involving multiple or overlapping keys amoung privilege levels have been left as future work and will not be discussed here.

IV. Scheme Security

A. Single Additional Noise

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.