

# Privileged Estimate Fusion With Correlated Gaussian Keystreams

Conference on Decision and Control (CDC) 2022

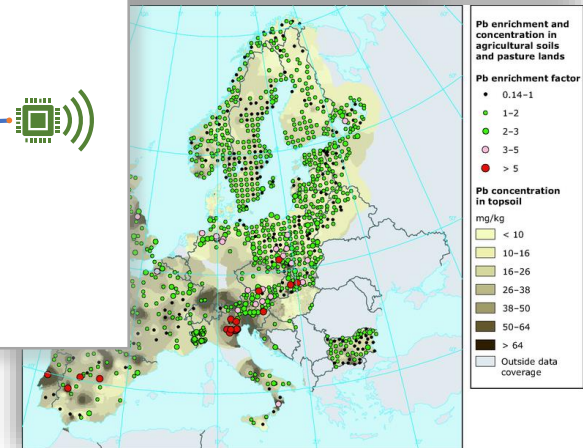
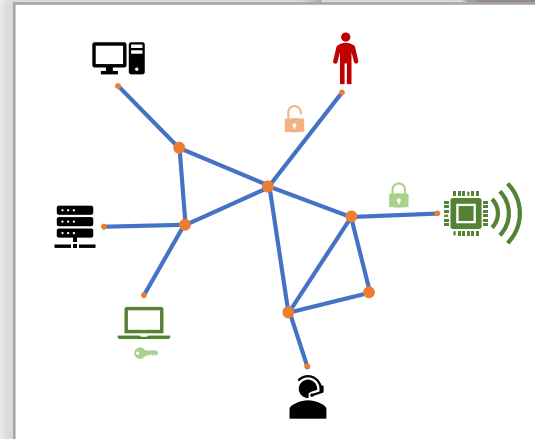
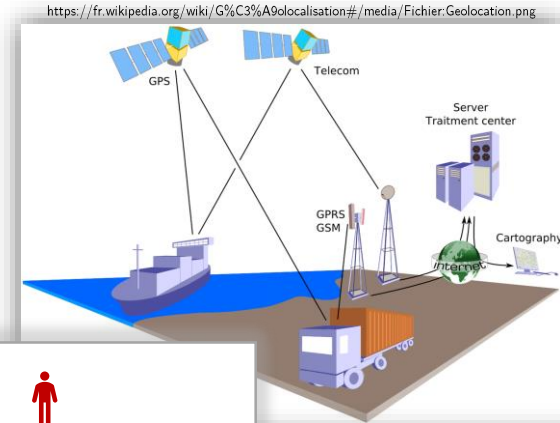
**Marko Ristic, Benjamin Noack**

Autonomous Multisensor Systems Group  
Institute for Intelligent Cooperating Systems  
Faculty of Computer Science  
Otto von Guericke University, Magdeburg

9.12.2021

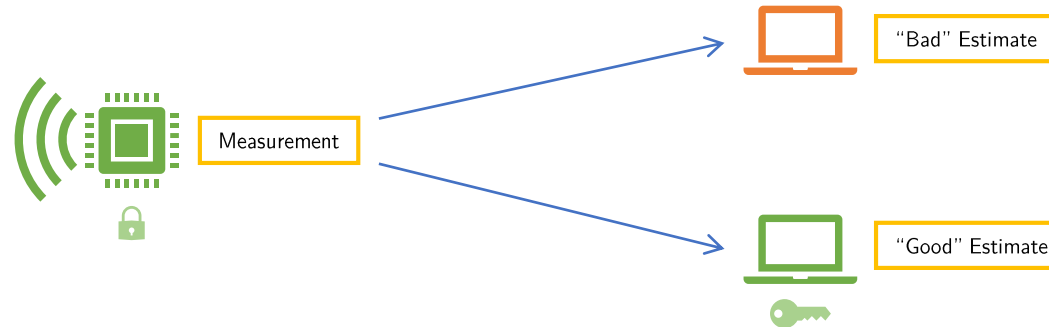


- Growing number of public networks
- Increasingly used by distributed sensors, IoT devices, cloud computing, etc
- Greater need for security guarantees
- Affected users
  - Private
  - Commercial
  - Government

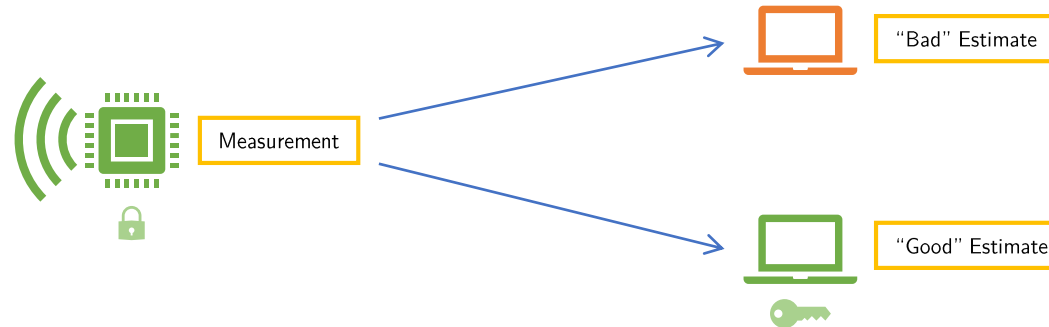


<https://www.eea.europa.eu/data-and-maps/figures/soil-contamination-by-heavy-metals>

- Public measurements useable for state estimation
- Trusted or special users may be granted *privilege*
- Privileged users should perform *better* than unprivileged ones



- Public measurements useable for state estimation
- Trusted or special users may be granted *privilege*
- Privileged users should perform *better* than unprivileged ones



- Security guarantee concerns proving the minimum difference in performance

- Add generated Gaussian keystream to measurements
- Anyone holding generation key can remove added noise

- Add generated Gaussian keystream to measurements
- Anyone holding generation key can remove added noise

- System

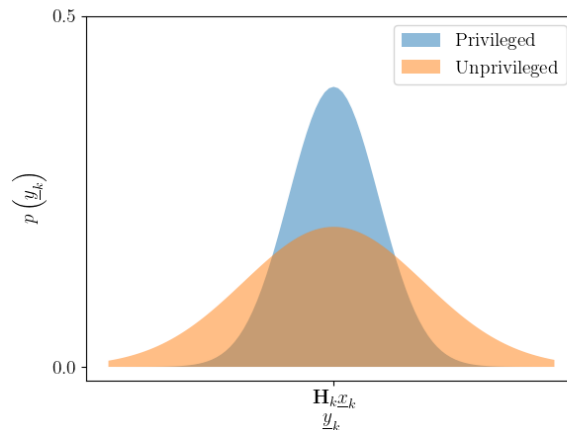
$$\underline{x}_k = \mathbf{F}_k \underline{x}_{k-1} + \underline{w}_k \quad \underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q}_k)$$

- Measurement

$$\underline{y}_k = \mathbf{H}_k \underline{x}_k + \underline{v}_k \quad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k)$$

- Modified measurement

$$\underline{y}'_k = \underline{y}_k + \underline{g}_k = \mathbf{H}_k \underline{x}_k + \underline{v}_k + \underline{g}_k \quad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k), \quad \underline{g}_k \sim \mathcal{N}(\underline{0}, \mathbf{Z})$$



- Algorithms

Setup  $(\mathcal{M}_S, \mathcal{M}_M, \kappa)$ ,  
Noise  $(\text{pub}, \text{sk}, k, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1, \dots, \underline{y}_k)$

- Definitions

*estimator*,  
 $\text{neglCov}_m(\kappa) : \mathbb{N} \rightarrow \mathbb{R}^{m \times m}$

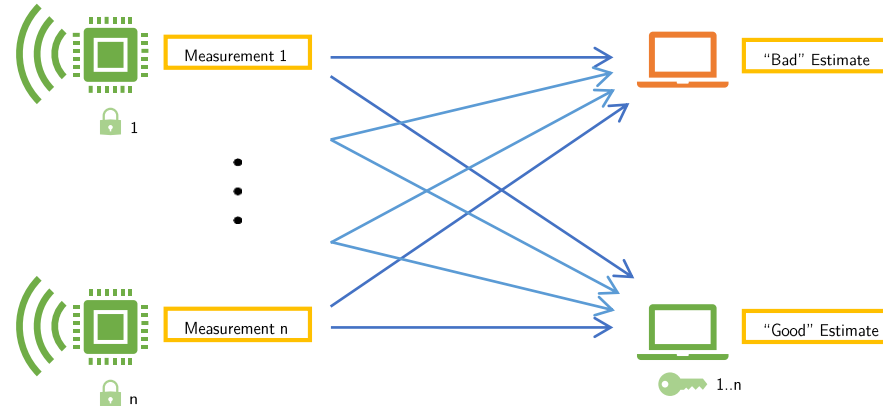
- Covariance Privilege

(Setup, Noise) meets  $\{\mathbf{D}_1, \mathbf{D}_2, \dots\}$ -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

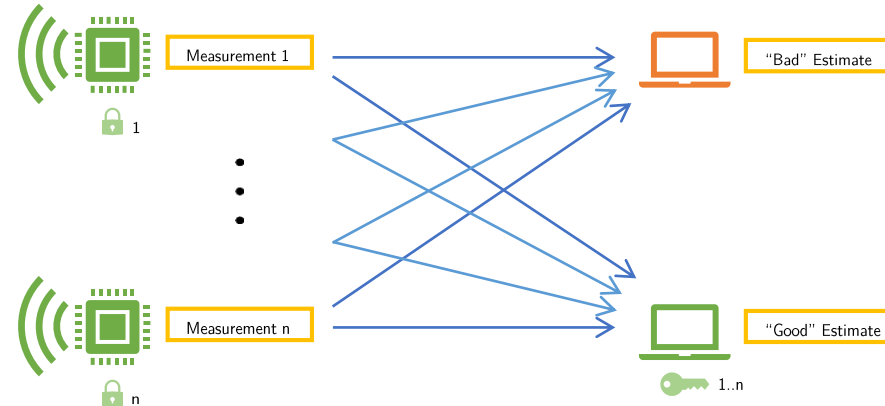
$$\begin{aligned} & \text{Cov} \left[ \mathcal{A} \left( k, \kappa, \text{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}'_1, \dots, \underline{y}'_k \right) - \underline{x}_k \right] \\ & - \text{Cov} \left[ \mathcal{A}' \left( k, \kappa, \text{pub}, \mathcal{M}_S, \mathcal{M}_M, \underline{y}_1,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

- Multiple privileged sensors each adding Gaussian keystore





- Multiple privileged sensors each adding Gaussian keystream



- Two ways of getting better estimates
  - Hold keys to remove added noises (desired)
  - Fuse more measurements (desired only when keys are held as well)

- Linear models considered
- Kalman Filter optimality in proofs

- System

$$\underline{x}_k = \mathbf{F}_k \underline{x}_{k-1} + \underline{w}_k \quad \underline{w}_k \sim \mathcal{N}(\underline{0}, \mathbf{Q}_k)$$

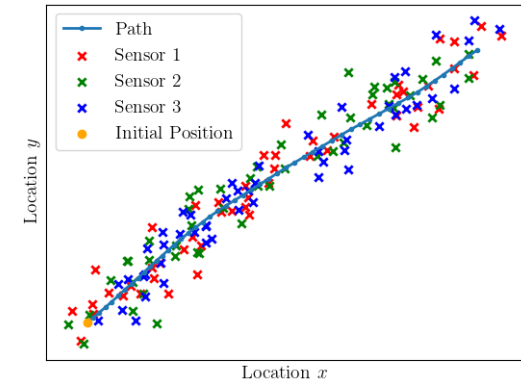
- Measurements

$$\underline{y}_{k,i} = \mathbf{H}_{k,i} \underline{x}_k + \underline{v}_{k,i} \quad \underline{v}_{k,i} \sim \mathcal{N}(\underline{0}, \mathbf{R}_{k,i}), \quad 1 \leq i \leq n$$

- Modified measurements and keys

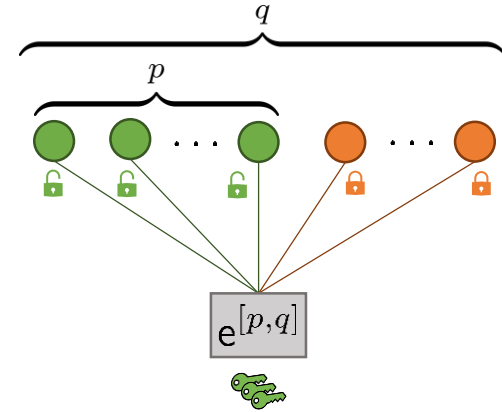
$$\underline{y}'_{k,i}, \text{ sk}_i \quad 1 \leq i \leq n$$

Example: Linear Constant Velocity Model ( $n = 3$ )



- Estimators can access  $q$  measurements ( $1 \leq q \leq n$ )
- Estimators have privilege  $p$  (# of keys) ( $0 \leq p \leq n$ )

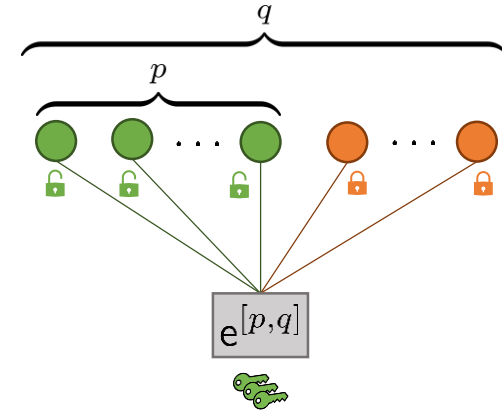
$e^{[\text{privilege, access}]}$



- Estimators can access  $q$  measurements ( $1 \leq q \leq n$ )
- Estimators have privilege  $p$  (# of keys) ( $0 \leq p \leq n$ )

$e^{[\text{privilege, access}]}$

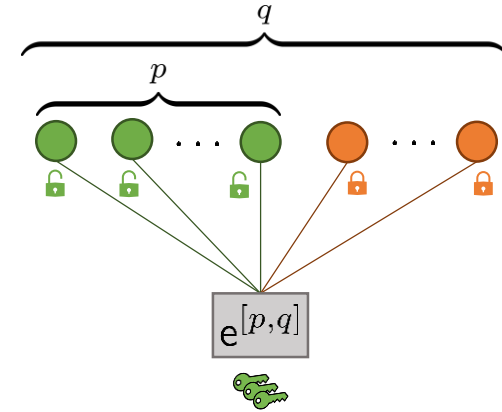
- Estimators have access to sequential measurements
- *All* measurements for which they hold a key are accessible



- Estimators can access  $q$  measurements ( $1 \leq q \leq n$ )
- Estimators have privilege  $p$  (# of keys) ( $0 \leq p \leq n$ )

$e^{[\text{privilege, access}]}$

- Estimators have access to sequential measurements
- *All* measurements for which they hold a key are accessible

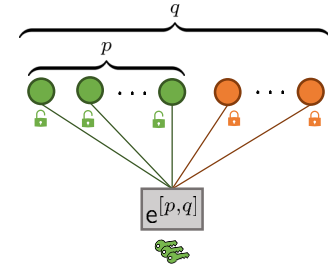


$e^{[0,q]}$  Access to:  $\underline{y}'_{k,i}, 1 \leq i \leq q$

$e^{[p,p]}$  Access to:  $\underline{y}'_{k,i}, \text{sk}_i, 1 \leq i \leq p$

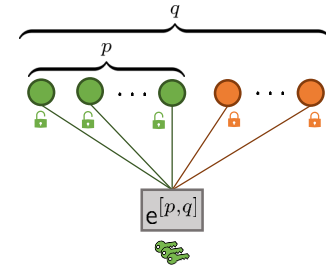
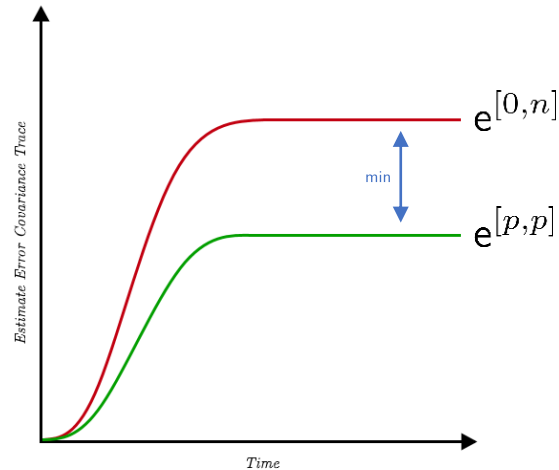
$e^{[p,q]}$  Access to:  $\underline{y}'_{k,i}, 1 \leq i \leq q \quad \text{sk}_j, 1 \leq j \leq p$

- Capture desired performance differences in multisensor environment



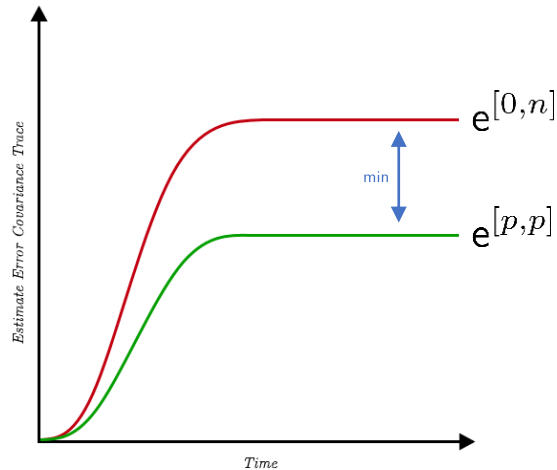
- Capture desired performance differences in multisensor environment

## Performance Loss Lower Bound

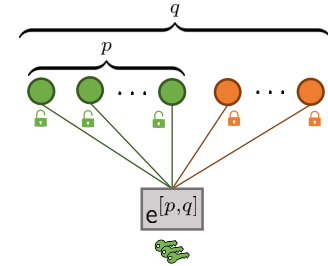
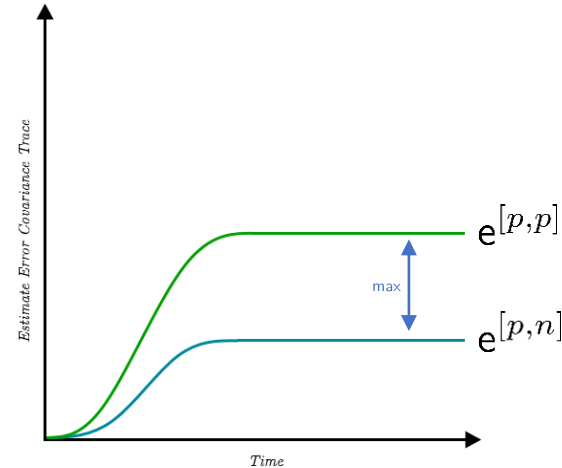


- Capture desired performance differences in multisensor environment

Performance Loss Lower Bound



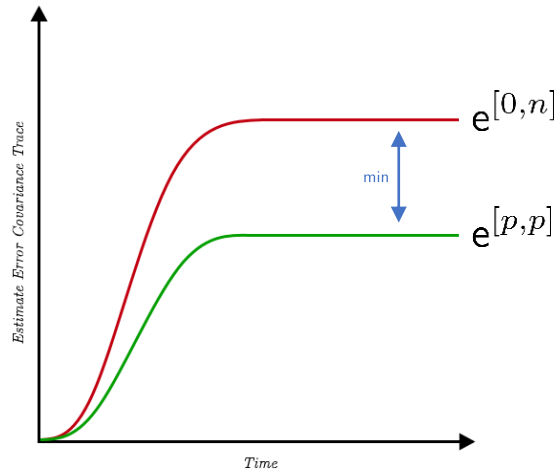
Performance Gain Upper Bound



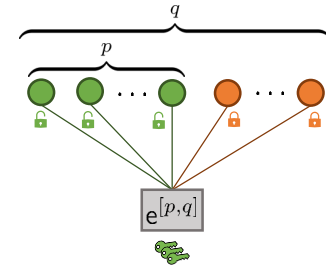
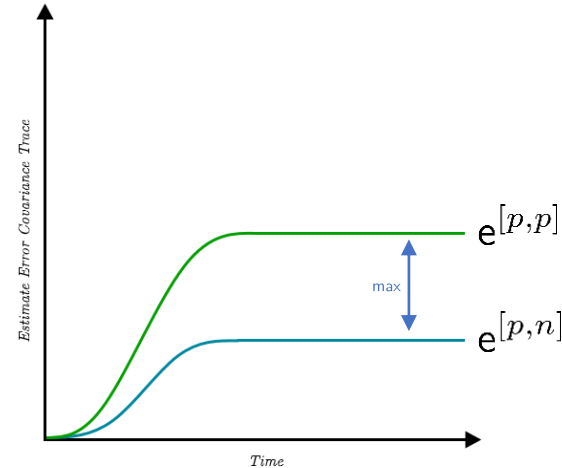


- Capture desired performance differences in multisensor environment

Performance Loss Lower Bound



Performance Gain Upper Bound



- Both bounds desired for each privilege  $p$

- Generate uniform keystreams from  $sk_i$  for  $1 \leq i \leq n$
- Correlated uniform keystreams with Box-Muller transform

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,n} \end{bmatrix} \sim \mathcal{N}(\underline{0}, \mathbf{S}^{(n)}) \quad \mathbf{S}^{(n)} = \overbrace{\begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}}^{n \text{ blocks}} + \begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}$$

Correlated component                      Uncorrelated component

- Generate uniform keystreams from  $sk_i$  for  $1 \leq i \leq n$
- Correlated uniform keystreams with Box-Muller transform

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,n} \end{bmatrix} \sim \mathcal{N}(\underline{0}, \mathbf{S}^{(n)}) \quad \mathbf{S}^{(n)} = \overbrace{\begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}}^{n \text{ blocks}} + \begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}$$

Correlated component                      Uncorrelated component

- Add generated keystreams to measurements

$$\underline{y}'_{k,i} = \underline{y}_{k,i} + \underline{g}_{k,i} = \mathbf{H}_{k,i} \underline{x}_k + \underline{v}_{k,i} + \underline{g}_{k,i} \quad \underline{v}_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_{k,i})$$

- Each added noise depends on multiple keys!
- Need to correctly reconstruct partial noises when  $p < n$
- Lower-triangular decomposition (e.g. Cholesky) in Box-Muller transform ensures

$$\underline{g}_{k,i} \text{ depends on } \text{sk}_j, 1 \leq j \leq i$$

- Each added noise depends on multiple keys!
- Need to correctly reconstruct partial noises when  $p < n$
- Lower-triangular decomposition (e.g. Cholesky) in Box-Muller transform ensures

$$\underline{g}_{k,i} \text{ depends on } \text{sk}_j, 1 \leq j \leq i$$

- Can reconstruct first  $p$  noises with  $\text{sk}_i, 1 \leq i \leq p$  exactly (recall sequential assumption)

$$\begin{bmatrix} \underline{g}_{k,1} \\ \vdots \\ \underline{g}_{k,p} \end{bmatrix} \sim \mathcal{N}(\underline{0}, \mathbf{S}^{(p)}) \quad \mathbf{S}^{(p)} = \overbrace{\begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}}^{p \text{ blocks}} + \begin{bmatrix} \mathbf{Y} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{Y} \end{bmatrix}$$

- Gaussian keystream indistinguishable from random without key
- Leads to three observable measurement models

- Gaussian keystream indistinguishable from random without key
- Leads to three observable measurement models

Notation

$$\mathbf{R}_k^{(1:q)} = \begin{bmatrix} \mathbf{R}_{k,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \ddots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{R}_{k,q} \end{bmatrix}$$

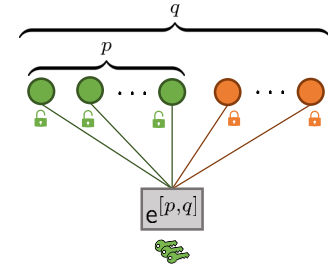
$$\bar{\mathbf{Z}} = \begin{bmatrix} \mathbf{Z} & \cdots & \mathbf{Z} \\ \vdots & \ddots & \vdots \\ \mathbf{Z} & \cdots & \mathbf{Z} \end{bmatrix}$$

$$\mathbf{e}^{[0,q]} \quad \underline{y}_k = \mathbf{H}_k^{(1:q)} \underline{x}_k + \underline{v}'_k \quad \underline{v}'_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k^{(1:q)} + \mathbf{S}^{(q)})$$

$$\mathbf{e}^{[p,p]} \quad \underline{y}_k = \mathbf{H}_k^{(1:p)} \underline{x}_k + \underline{v}'_k \quad \underline{v}'_k \sim \mathcal{N}(\underline{0}, \mathbf{R}_k^{(1:p)})$$

$$\mathbf{e}^{[p,q]} \quad \underline{y}_k = \mathbf{H}_k^{(1:q)} \underline{x}_k + \underline{v}'_k \quad \underline{v}'_k \sim \mathcal{N}\left(\underline{0}, \begin{bmatrix} \mathbf{R}_k^{(1:p)} & \mathbf{0} \\ \mathbf{0} & \mathbf{S}^{(q-p)} - \bar{\mathbf{Z}} (\mathbf{S}^{(p)})^{-1} \bar{\mathbf{Z}} + \mathbf{R}_k^{(p+1:q)} \end{bmatrix}\right)$$

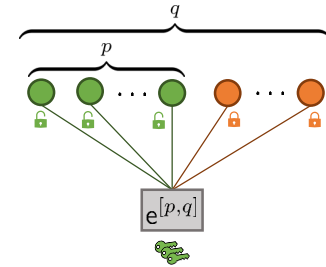
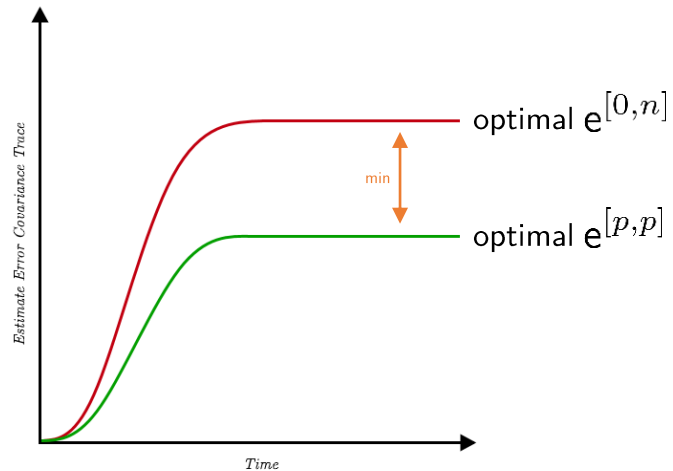
- Exact linear models mean optimal estimates





- Exact linear models mean optimal estimates

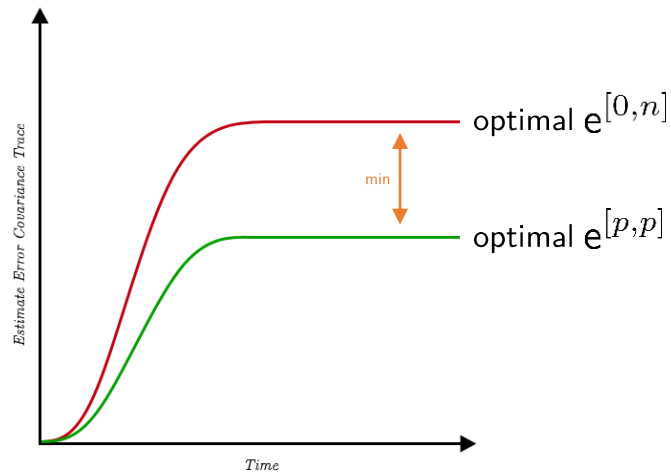
## Performance Loss Lower Bound



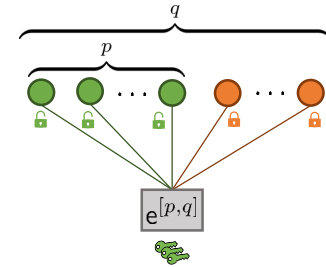
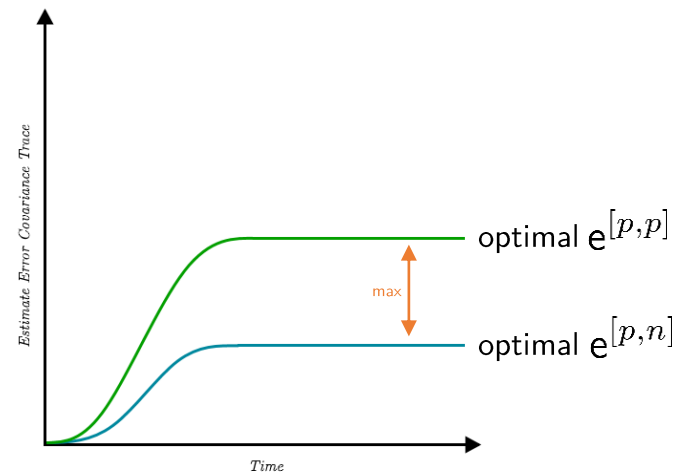
$$\mathbf{P}_0 = \mathbf{0} \implies \text{Lowest possible } \text{tr}(\mathbf{P}_k)$$

- Exact linear models mean optimal estimates

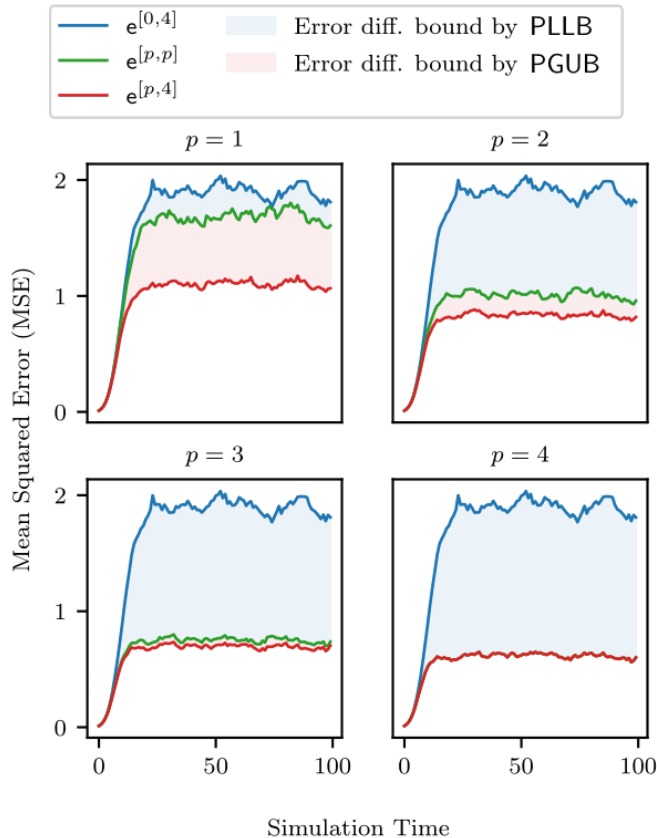
Performance Loss Lower Bound



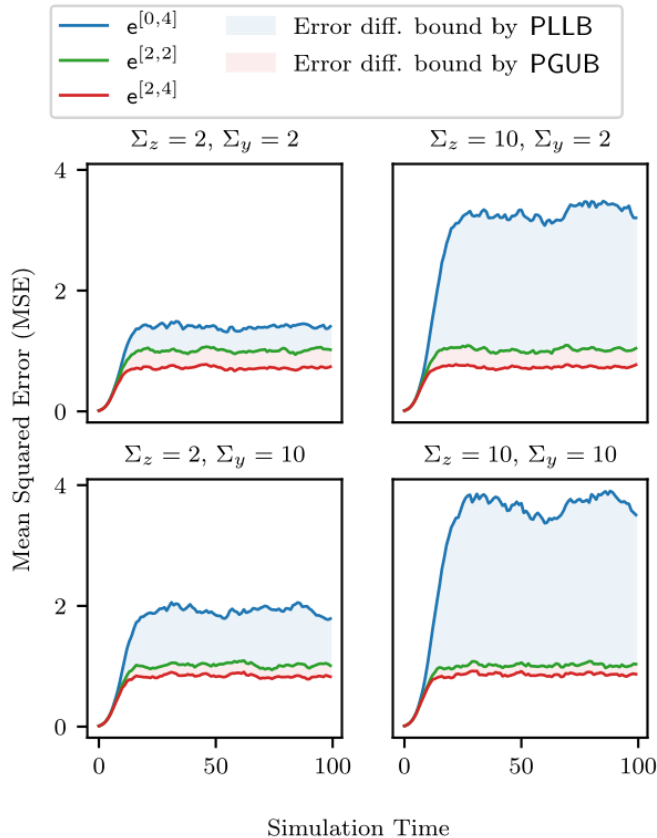
Performance Gain Upper Bound



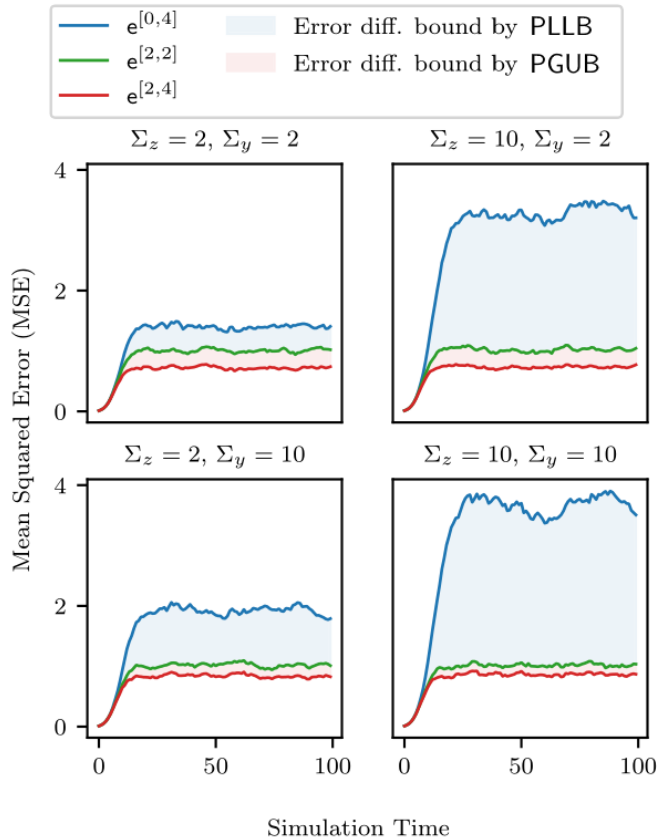
$$\mathbf{P}_0 = \mathbf{0} \implies \text{Lowest possible } \text{tr}(\mathbf{P}_k)$$



- $n = 4$
- Fixed fully correlated component  $\mathbf{Z}$  and uncorrelated component  $\mathbf{Y}$



- $n = 4$
- Varied  $\mathbf{Z} = \Sigma_z \times \mathbf{I}$  and  $\mathbf{Y} = \Sigma_y \times \mathbf{I}$



- $n = 4$
- Varied  $\mathbf{Z} = \Sigma_z \times \mathbf{I}$  and  $\mathbf{Y} = \Sigma_y \times \mathbf{I}$
- Effect of  $\mathbf{Z}$  and  $\mathbf{Y}$  on bounds?

- Search for correlation matrix parameters that affect bounds independently
- Relaxations of sequential assumption



Phone: +49 391 67 57591  
Email: [marko.ristic@ovgu.de](mailto:marko.ristic@ovgu.de)  
Web: <https://ams.ovgu.de>

## Thank you!