Master's Project

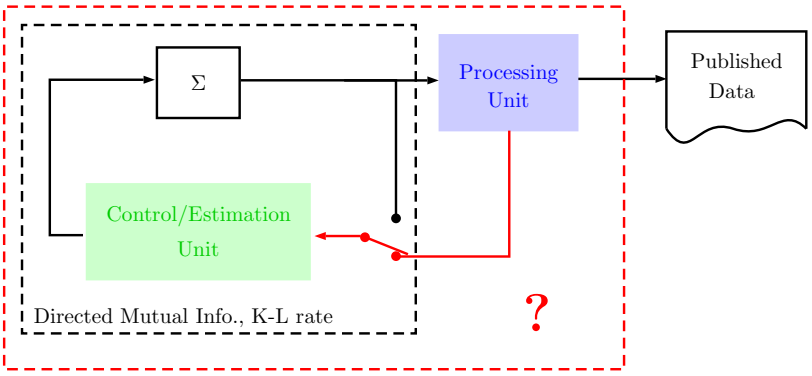
REGELUNGS- UND AUTOMATISIERUNGS-TECHNIK

Project Title: Exploring Privacy Notions for Dynamical Systems

Background: The sharing of user data with service providers such as electricity companies and Internet search providers often leads to more accurate and better service delivery. However, collecting frequent measurements about individual users can also be regarded as an invasion of privacy. Methods which preserve the privacy of users, while still allowing users to benefit from such services, have attracted significant recent attention in the scientific community.

In the statistical database field, the notion of differential privacy has been proposed and studied, mostly for static systems or systems with uncorrelated data. Ideally, privacy will be ensured if the probability of inferring private data, given the publicly available data, is low enough. To achieve this goal, differential privacy mechanisms guarantee that a wide range of private information lead to the same public data. Whilst recent work has attempted to extend the notion of differential privacy to dynamical systems [1], this notion may not be the most suitable one when there is correlated data. In this project we aim to explore new privacy notions that can prevent the individual's information being inferred from the information released by a dynamical system, taking into account the inherent data correlations in dynamical systems.

Project: We focus on linear discrete-time dynamical systems. To derive privacy measures for such systems we will adopt an information theoretic approach. As a first step, we will study the suitability of using the Kullback-Leibler rate metric [2] and directed mutual information [3] between private data and public data. These two notions are well developed for conventional dynamical systems with feedback, but have not been used to deal with privacy issues when public information is released.



Prerequisites: A strong mathematical background. Knowledge of control theory and stochastic processes. Knowledge of or willingness to learn information theory.

Contact: Prof. Daniel Quevedo, Dr. Alex Leong. `dquevedo@ieee.org, alex.leong@upb.de`

References

[1] J. L. Ny and G. J. Pappas, "Differentially Private Filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, feb 2014.

[2] S. Yu and P. G. Mehta, "The Kullback Leibler rate pseudo-metric for comparing dynamical systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 7, pp. 1585–1598, 2010.

[3] J. L. Massey, "Causality, feedback and directed information," in *International Symposium on Information Theory and its Applications*, 1990, pp. 303–305.