Thesis or Project: Integrity in encrypted control

- Verifiable computations for encrypted state feedback -

Task description

In many cyberphysical systems, solving the control task is outsourced due to often heavy computational demands, or because the solution depends on other participants. This raises privacy concerns to which the young research field of encrypted control provides answers. In order to keep the data private to eavesdroppers, the communication can be encrypted using standard cryptography tools. However, the control cloud operator and malicious agents, that potentially hacked the cloud, can access the private data, such as control inputs and system outputs, because they are decrypted for the controller evaluation. Homomorphic encryptions provide a solution to this privacy concern, as they allow to evaluate the control function on the encrypted data. This encrypted control loop is depicted in Figure 1.

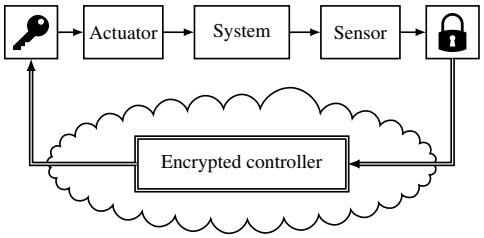

Figure 1: Encrypted controller for cyberphysical systems.

The current literature in this research area mainly focus on the confidentiality of data. However, one should also guarantee the integrity of calculations, i.e., whether the control law is evaluated correctly and no malicious agent has modified the result.
The thesis or project aims for combining confidentiality and integrity for a relatively simple control scheme, namely static state feedback. For this setting, [1] proposes a plaintext solution based on verifiable computations. The main goal of this thesis is to extend the approach by implementing it using a partially homomorphic encryption scheme.

Your Profile

Ideally, your profile should match some items listed below:

- Programming skills in Matlab or (preferrable) Python
- Linear algebra fundamentals
- Basic understanding of control theory
- Interest in cybersecurity

Still, do not hesitate to apply for the thesis even if you do not yet have these skills. Appropriate support can be provided by the supervisor.

Interested?

If you are interested in this thesis, please contact us at janis.adamek@tu-dortmund.de. Make sure to include relevant information about yourself and your course of studies as detailed here.

References

[1] Jung Hee Cheon, Dongwoo Kim, Junsoo Kim, Seungbeom Lee, and Hyungbo Shim. Authenticated computation of control signal from dynamic controllers. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3249–3254. IEEE, 2020.