Master degree internship

Advanced encrypted command laws

With the development of cloud computing - i.e. the delegation of data processing to a remote server - in many modern control systems (smart grids, intelligent transport systems, robotics applications, etc.), security issues have become increasingly important. Securing cyber-physical systems is therefore a major challenge for the future. Indeed, many types of attack are aimed at altering and degrading the behavior of systems; for example, eavesdropping attacks compromise the computing server and retrieve unencrypted data, remote control attacks alter the server's calculations and send malicious commands to the system [1]. One solution to this problem is to encrypt the data and perform operations directly on the encrypted data. This technique can be applied using the new homomorphic encryption algorithms, which satisfy the following properties:

$$\mathrm{Enc}(x_1 + x_2) = \mathrm{Enc}(x_1) \oplus \mathrm{Enc}(x_2) \quad \text{and} \quad \mathrm{Enc}(x_1 x_2) = \mathrm{Enc}(x_1) \otimes \mathrm{Enc}(x_2),$$

where Enc is the encryption function. Today, the major challenges are to extend the applicability of these encryption methods to control systems, and to certify their robustness (stability, precision and security).

In the Prisme laboratory, the security of cyber-physical systems is an important area of work (for example, sporadic sampling methods linked to interval observers have shown the resilience of linear systems to a Denial of Service attack). In the literature, works [2, 3] have highlighted the possibility of controlling systems with HE algorithms. However, the techniques proposed are applicable to integer values, and their application to real data is only possible through quantization, which leads to accuracy errors. The objectives of this internship are:

1. Explore the implementation of new algorithms, such as [4], and evaluate their performance in controlling dynamical systems.

2. Study the stability, convergence and robustness properties of encrypted control laws for nonlinear systems.

The first step is to implement various clear control laws (linear-quadratic, predictive, observer-based) for autonomous linear systems. Then, the same laws will be implemented with encryption (the encryption/decryption algorithm will be provided), see [5]. Then, by measuring the performance of the various encrypted control laws - in terms of tracking quality, computation time, robustness to uncertainties and security - we will demonstrate stability and convergence results for the controls constructed. Finally, using linearization techniques (extension, class equivalence, etc.), the results obtained will be applied to non-linear systems (the case of a mobile robot).

Keywords: encryption, command, observer, robustness

Timothée Schmoderer, Polytech Orléans, 8 rue Léonard de Vinci, 45000 Orléans
Tél : 02 38 41 73 34 email : timothee.schmoderer@univ-orleans.fr

Skills:

- Master 2 student in automatic control or applied mathematics with good knowledge in closed-loop control.
- Solid knowledge in programming: Matlab & Simulink or Python or C++.

How to apply: Send a cover letter, a full CV, grades -even incomplete- for the last two year (including the current academic year), as well as a recommendation letter to:

timothee.schmoderer@univ-orleans.fr
estelle.courtial@univ-orleans.fr

Candidate recruitment subject to ZRR approval.

Application deadline: **January 26, 2024**
Location: Laboratoire Prisme, site Vinci at Orléans, France.
Duration of the internship: March 2024 – August 2024.
Team: Automatic control (IRAUS Departement).
Mentors: Timothée Schmoderer & Estelle Courtial.

[1] Riccardo MG Ferrari and André MH Teixeira. *Safety, security and privacy for cyber-physical systems*. Springer, 2021.

[2] Moritz Schulze Darup, Adrian Redder, Iman Shames, Farhad Farokhi, and Daniel Quevedo. "Towards encrypted MPC for linear constrained systems". In: *IEEE Control Systems Letters* 2.2 (2017), pp. 195–200.

[3] Yankai Lin, Farhad Farokhi, Iman Shames, and Dragan Nešić. "Secure control of nonlinear systems using semi-homomorphic encryption". In: *2018 IEEE Conference on Decision and Control (CDC)*. IEEE. 2018, pp. 5002–5007.

[4] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. "Homomorphic encryption for arithmetic of approximate numbers". In: *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Proceedings, Part I 23*. Springer. 2017, pp. 409–437.

[5] Hung Nguyen, Binh Nguyen, Hyung-Gohn Lee, and Hyo-Sung Ahn. "Encrypted Observer-based Control for Linear Continuous-Time Systems". In: *arXiv preprint arXiv:2303.00963* (2023).

Timothée Schmoderer, Polytech Orléans, 8 rue Léonard de Vinci, 45000 Orléans
Tél : 02 38 41 73 34 email : timothee.schmoderer@univ-orleans.fr