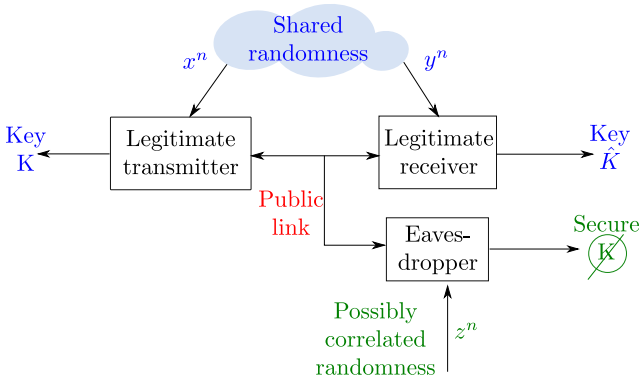
Graduate Internship position

Polar coding based secret key generation

Context and research statement

Secret key generation from shared randomness, also termed *information theoretic key generation*, allows to extract a secret key from shared randomness between two legitimate nodes in the presence of an eavesdropper which intercepts all key-agreement messages as shown in the figure below. In this key generation scheme, shared randomness consists in a pair of (strongly) correlated random physical processes observed by both legitimate nodes.



Typical sources of shared randomness can be Physically Unclonable Functions (PUF) [1], entangled photons as in Quantum Key Distribution (QKD) [2], or even wireless channel signatures reciprocity as in LTE or 5G communications [3].

In this internship, the focus will be on the analysis and implementation of a particular state-of-the-art **secret key generation** scheme based on polar codes [4] which combines principles from information theoretic security and design criteria from error correction coding. The design will account for a variety of models for the sources of common randomness (Gaussian additive noise, binary symmetric sources, erasure sources, ...).

The research assignment will consist first in a bibliographic search about the sources of common randomness and key generation schemes and an analysis of the design criteria of theoretical and practical polar codes for secret key generation. Then, a security analysis will be carried out through the computation of the information leakage of the generated key. The results will then be implemented using Matlab (or python), and possibly, a system level implementation on the locally deployed software-defined radio platform RALF.

References

[1] L. Kusters, T. Ignatenko, F. M. Willems, R. Maes, E. van der Sluis, and G. Selimis, "Security of helper data schemes for sram-puf in multiple enrollment scenarios," in *2017 IEEE International Symposium on Information Theory (ISIT)*, 2017, pp. 1803–1807.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *2017 IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, 1984, pp. 1803–1807.

[3] C. L. Kameni Ngassa, R. Molière, F. Delaveau, A. Sibille, and N. Shapira, "Secret key generation scheme from WiFi and LTE reference signals," *Analog Integrated Circuits and Signal Processing*, Mar. 2017. [Online]. Available: https://hal.telecom-paris.fr/hal-02287588

[4] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," in *2013 IEEE Information Theory Workshop (ITW)*, 2013, pp. 1–5.

Candidate profile and application

Applicants should be last-year research master (or/and engineer) students. A strong background in digital communications, signal processing, and applied mathematics is required since the research assignment requires tools from information theory and error correction coding. Good communication skills in English are necessary (written and oral), as well as good development skills (Matlab, C++). Applications from candidates familiar with digital communications, information theory or error correction coding are particularly encouraged.

Applications (CV, cover letter, academic records) are to be addressed to {meryem.benammar,damien.roque}@isae-supaero.fr

About

ISAE-Supaéro is a leading european institute in system designs for aeronautical and space applications. The internship will take place in the Department of Electronics, Optronics and Signal processing (DEOS) of ISAE-Supaéro. Among the department's main research interests lies the design of "satellite communication systems with high spectral efficiency and enhanced security", and this internship is directly related to this research activity.

- Financial grant, accommodation and food services are available on the campus of ISAE.
- Dates and duration: between March and October 2023 (5 to 6 months).
- **Application deadline: open until January 31st, 2023**.