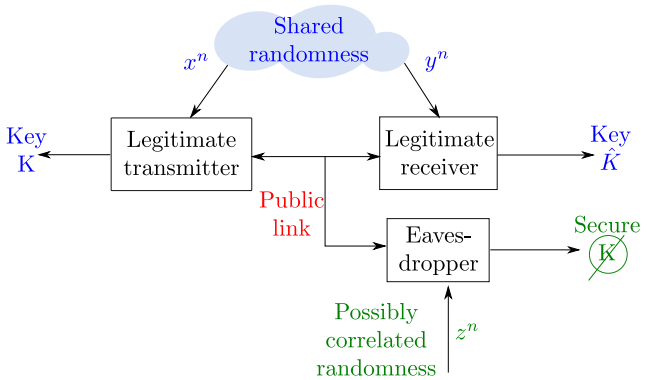
PhD thesis proposal:
"Secret Key Generation from shared randomness"

1 Context

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]. Unlike cryptographic secret key generation which relies on provably hard-to-invert mathematical transformations, information theoretic key generation distills a secret key from a probabilistic asymmetry of information entailed by the statistical correlation of the shared randomness processes.

Irrespective of the source of shared randomness, provably secure key generation schemes can be classified into those based on *Slepian-Wolf source coding*, and those based on *Wiretap channel coding*. However, both families of key generation schemes rely on mathematical objetcs, namely random codes, which do not have a practical implementation, and hence, both schemes have long remained and deemed theoretical.

Some attempts were made for the construction of practical key generation schemes (channel reciprocity [3], PUF [4]. However, these works present two main limitations.

First, they often base their security proof on heurisitc measures and not on an information theoretic argument. Besides, these works fail to account for the effect of a possibly correlated shared randomness at the eavesdropper, and hence, do not fully assess the *quality* of the shared randomness between the legitimate users.

Hence, in this thesis, the focus will be on the implementation of practical secret key generation schemes while characterizing formally the properties of the source of shared randomness and their effect on the security level. Besides, and implementation using real transmitters and receivers (USRP) will be targetted to evaluate the performances of the derived secret generation schemes.

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] O. Günlü and R. F. Schaefer, "An optimality summary: Secret key agreement with physical unclonable functions," *Entropy*, vol. 23, no. 1, 2021. [Online]. Available: https://www.mdpi.com/1099-4300/23/1/16

2 Research team

As part of the University of Toulouse, ISAE-SUPAERO is a public higher education and research institute focused on aeronautical and aerospace applications. The Department of Electronics, Optronics and Signal processing (DEOS) is leading research in various electrical engineering topics among which are "secure and high spectral efficiency satellites and aeronautical communications". Our webpage: http://isae.fr/deos/comit. The main advisor of the thesis will be Meryem Benammar, associate professor, whose research activities lie mostly in information theory, with applications to communication engineering and statistical learning theory. The thesis will be held under the co-direction of Damien Roque, professor, whose research interests are in the field of signal processing and waveforms/receivers design.

3 Candidate profile and application

Applicants should be graduated master (or/and engineer) students. A strong background in applied mathematics is required since the research assignment requires tools from information theory and coding theory. A strong background as well in digital communications, information theory and/or coding theory are good assets for the application. Good communication skills in English are necessary (written and spoken), as well as good development skills (Python, Matlab, ...).

- Applications (CV, cover letter, academic records) are to be addressed to {meryem.benammar,damien.roque}@isae-supaero.fr
- Dates and duration: oct-2023 → oct-2026 (36 months)
- **Application deadline: open until March 20th, 2023**.