PhD thesis proposal

Physical layer security: secure communications and key generation

1 Context

Since its introduction in one of Shannon's most celebrated papers [1], adn later Wyner [2] and Csiszár Körner [3], physical layer security has proved to be a promising means of **securing communications** by exploiting the inherent **non-reproducible randomness and asymmetry** in the communication links (noisy channels, fading channels, ...) in order to create advantage of the legitimate users over the eavesdroppers. Unlike cryptographic based methods, which are applied at the upper layers of the communication protocols stack, security at the physical layer is resilient to any computational power of the eavesdropping nodes, since it does not rely on the algebraic hardness of key reproduction, e.g, prime numbers based factorization.

Whilst long regarded as a purely theoretic form of security inspired from information-theoretic analysis, in the last decades, physical layer security has substancially matured, and constructions of **secure transmission** and **secret key generation** schemes based on channel randomness and asymmetry are now provably implementable for some simple communication scenarios, e.g., Point-to- Point Binary Erasure Channels (BEC) or Binary Symmetric Channels (BSC). These constructions consist in the so-called wiretap codes, [4,5], which are error correction codes judiciously designed to create advantage of the legitimate receivers over the eavesdroppers and thus, secure the communication.

Yet, wiretap codes constructions for more complex scenarios (multiple users, fading channel, distributed key generation,...) remain, to date, not fully explored and understood.

The focus of this thesis will be the design of practical physical layer security solutions for a variety of secure communications and secret key generation scenarios. These solutions will be inspired from the optimal information theoretic security schemes and will be analyzed and built from a error correction coding perspective, with possible applications in wireless communications or satellite and aeronautical communications.

2 Research program

The research assignment will consist in combining theoretical foundations of information theoretic security, with code analysis inspied from error correction coding theory, and realistic implementation contraints to design different physical layer security solutions. The scenarios of interest

include, but are not limited to,

- A point to point communication channel with one eavesdropper and various channel assumptions: the reasearch assignment herein will consist in a thorough state of the art for information theoretic basics of physical layer security and fundamentals of error correction coding. This should allow to derive optimal design criteria of wiretap codes for a simple scenario with one legitimate user and one eavesdropper under simplistic channel assumptions (Gaussian, BSC, BEC,...)

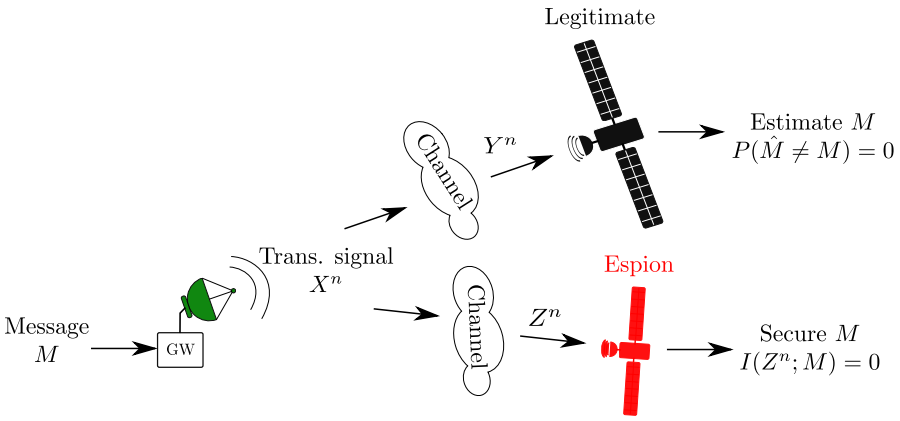

Figure 1: Single user / single eavesdropper communication scenario

- Multi-user communication networks with one or multiple eavesdroppers. In this part of the thesis, we will investigate the design of mutli-terminal wiretap codes where advanced interference mitigation schemes (non-orthogonal access) will be combined with security constraints for the disgn of the wiretap code. Applications to a 2-user wiretap Broadcast Channel (BC) with one eavesdropper, for instance, will be considered to start with. Other extensions can be investigated as well.

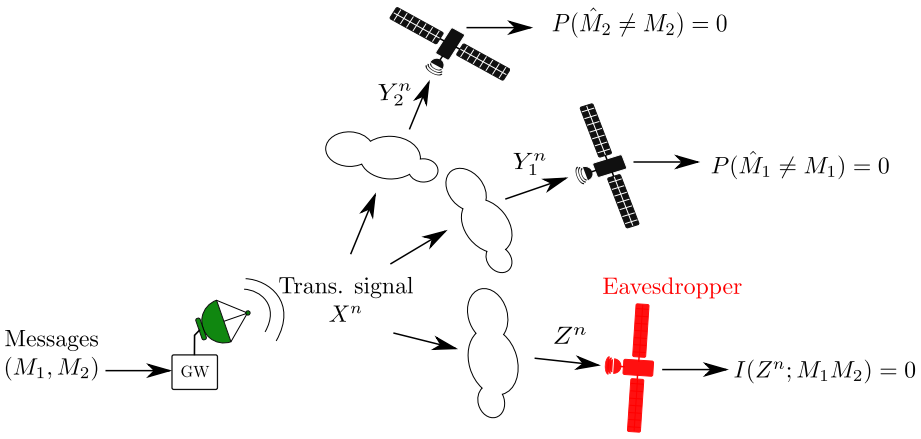

Figure 2: 2-user Wiretap Broadcast Channel with one eavesdropper

- Distributed key generation based on wiretap network codes or distributed compression schemes. In this part of the thesis, applications of wiretap codes to secure key generation will be investigated for both a basic scneario with two nodes and one eavesdropper,

and more complex multi-user settings. Applications of the obtained result will be targeted towards networks of Physically Unclonable Functions (PUFs) [6] or Quandtum Key Distribution (QKD)[7].

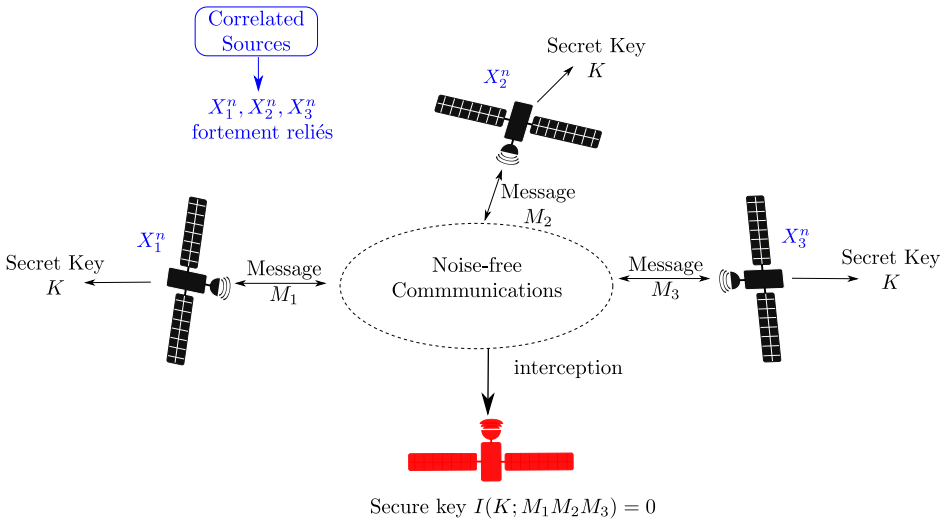

Figure 3: Distributed secret key generation

3 Research team

ISAE-Supaéro is a leading institue in applied research for aeronautical and aerospace engineering. The Department of Electronics, Optronics and Signal processing (DEOS) is leading research in various electrical engineering topics amongst which are " secure and high spetral efficiency sattelites and aeronautical communications".

The main advisor of the thesis will be Meryem Benammar, associate profession in DEOS, whose researche activities are most in information theory, with applications to various secure or non secure communication and data compression scenarios, as well as fundamental aspects of error correction coding (error exponents, code convergence analysis, ...).

The thesis will be partly co-advised by Tarik Benaddi, associate professor in IMT-Atlantique Toulouse site, whose research activities are strongly related to error correction code design, ranging from theoretic solutions, to simulation and implementation in realistic settings.

The thesis will be held under the direction of Jérôme Lacan, professor in ISAE-Supaéro, who has expertise in various error correction coding related topics, including errasure codes, and in security and cryptography.

4 Candidate profile and application

Applicants should be graduated master (or/and engineer) students. A strong background in digital communications, signal processing, and applied mathematics is required since the research assignement 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,jerome.lacan}@isae-supaero.fr, and tarik.benaddi@imt-atlantique.fr.
- Dates and duration: between September 2018 and September 2021 (36 months)
- **Application deadline: open until Late June 2018**.

5 References:

[1] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech- nical Journal, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wiretap channel," Bell Labs Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE transactions on information theory, vol. 24, pp. 339–348, 1978.

[4] M. Hayashi and R. Matsumoto, "Construction of wiretap codes from ordi- nary channel codes," in 2010 IEEE International Symposium on Information Theory, 13-18 June 2010, pp. 2538–2542.

[5] O. O. Koyluoglu and H. El Gamal, "Polar coding for secure transmission and key agreement," IEEE Transactions on Information Forensics and Security, vol. 7, no. 5, pp. 1472–1483, 2012.

[6] M. Alioto, A. Alvarez, "Physically Unclonable Function database," [Online]. Available: http://www.green-ic.org/pufdb.

[7] C. H. Bennett and G. Brassard. " Quantum cryptography: Public key distribution and coin tossing". In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8. New York, 1984