PhD position @ ISAE-SUPAERO

Physical layer security: secure communications and key generation

Thesis advisors: Jérôme Lacan (ISAE/DISC), Meryem Benammar (ISAE/DEOS)

Contact: Jerome.Lacan@isae-supaero.fr Meryem.Benammar@isae-supaero.fr

Application deadline: 31/01/2018

Scientific domain: Telecommunications, Cybersecurity, Information Theory

Keywords: security, physical layer, channel randomness, key generation, PUFs, wiretap codes

Summary : Since its introduction in one of Shannon's most celebrated papers [1] and its elaboration by Wyner [2] and Csiszár & Körner [3], physical layer security has proved to be a promising means of securing communications and generating random secret keys by exploiting the inherent non-reproducible randomness in either the communication links (noisy channels, fading channels, quantum optical channels ,...) or some physical processes involved in the communication (S-RAM units, Ring Oscillators, ...).

Unlike purely cryptographic methods which are deployed in the higher layers of the communication stack, physical layer security schemes are not prone to the computation powers of the eavesdropping nodes; they do not rely on the assumption that some operations are hard to be performed at the eavesdropper such as factorization in prime numbers. As such, they are more robust to the continuous advent of more powerful computing units.

Whilst long regarded as a purely theoretic form of security, in the last decades, physical layer security has substantially matured and constructions of secure transmission schemes based on channel randomness (wiretap codes [4, 5]) as well as key generation schemes based on physically unclonable functions (PUFs, [6, 7]) are now feasible and provably implementable for basic point-to-point settings and a few specific communication channels.

Yet, more realistic constructions with multiple nodes, with arbitrary communication channels, and distributed key generation schemes are still missing and constitute a promising line of work to empower the large scale implementation of physical layer security.

In this thesis, the focus will be on the design of physical layer security schemes for both secure communications and random key generation for such realistic settings. This will be performed by means of bridging deep theoretical understanding from information theoretic security, in order to characterize optimal theoretic secure mutli-terminal coding schemes, and design considerations from error correction coding theory, so as to build real codes approaching the optimal ones, and, eventually, thorough system level validations in order to assess the performance of the designed codes in realistic scenarios.

Applications of the obtained results may be found in satellite communications [8] (possibly with optical links) and wireless communications [9], and strong interactions with cryptography will be enabled by the secret key generation schemes through the design of PUFs.

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, no. 3, 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] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in Proceed- ings of the 6th ACM conference on Computer and communications security. ACM, 1999, pp. 28–36.

[7] C. Bösch, J. Guajardo, A.-R. Sadeghi, J. Shokrollahi, and P. Tuyls, “Efficient helper data key extractor on fpgas,” Cryptographic Hardware and Embedded Systems-CHES 2008, pp. 181–197, 2008.

[8] A. Vazquez-Castro and M. Hayashi, “Information theoretic physical layer security for satellite channels,” in 2017 IEEE Aerospace Conference, 4-11 March 2017, pp. 1–14.

[9] H. V. Poor and R. F. Schaefer, “Wireless physical layer security,” Proceedings of the National Academy of Sciences, vol. 114, no. 1, pp. 19–26, 2017.