Proposition de thèse ISAE-SUPAERO

Sécurité de la couche physique: Communications sécurisées et génération de clés

Directeurs de thèse : Jérôme Lacan (ISAE/DISC), Meryem Benammar (ISAE/DEOS)

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

Date limite de candidature : 31/01/2018

Domaine scientifique : Télécommunications, cyber-sécurité, théorie de l'information

Mots-clés : Sécurité, couche physique, aléa du canal, génération de clés, PUFs, codes Wiretap

Résumé : La sécurité de la couche physique a été introduite dans les travaux célèbre de Shannon [1] et de Wyner [2] et Csiszár Körner [3] et s'est avérée être un moyen prometteur pour la sécurisation des communications et la génération de clés aléatoires. Cette forme de sécurité exploite le caractère aléatoire et non-reproductible des canaux de communication (tels que les canaux à bruit additif, les canaux à évanouissements, les canaux optiques quantiques, ...) ainsi que de processus physiques intervenants dans la chaîne de communication (unités S-RAM, Ring Oscillators, ...)

Par opposition aux méthodes purement cryptographiques qui, elles, sont appliquées aux couches supérieures de la pile de commmunication, la sécurité de la couche physique est inconditionnelle par rapport aux capacités de calcul des noeuds espions car elle ne repose pas sur l'hypothèse que certaines opérations puissent être complexes , telles que la factoriation en nombres premiers. A cet effet, la sécurité de la couche physique est robuste vis à vis de l'amélioration continuelle des capacités de calcul ce qui justifie son grand intérêt.

Longtemps considérée comme une forme de sécurité relativement conceptuelle, la sécurité de la couche phyisque a connu un regain d'intérêt sur les dernières décennies, et a atteint un degré de maturité tel que des schémas sécurisés de transmission de données basés sur les codes wiretap [4,5] ou encore des schémas de génération de clés aléatoires basés sur les PUFs [6,7] (physically unclonable function) sont désormais faisables, et implémentés.

Toutefois, ces solutions sont encore spécifiques à des scénarios de communication point-à-point et pour uniquement quelques canaux de communications. La construction de schémas plus génériques en termes de nombre d'utilisateurs , de nature des canaux de communication et aussi en terme de schémas distribués de génération de clés constitue un axe de recherche conséquent et vital pour le déploiement de la sécurité de la couche physique à grande échelle.

Cette thèse portera sur la construction de schémas de la sécurité de la couche physique pour des scnéarios de communication réalistes. L'approche sera de combiner les outils théoriques issus de la sécurité en théorie de l'information , afin de caractériser les schémas théoriques optimaux, à des critères de conception issus de la théorie du codage correcteur d'erreurs , afin de construire des codes qui permettent d'approcher les limites théoriques, et, ensuite, de valider les schémas proposés par des simulations au niveau système .

Les applications des résultats obtenus peuvent cibler les communications satellites [8], avec ou sans liens optiques, ainsi que les communications sans fil [9] au sens plus large. Les schémas de génération de clés seront, eux, destinés à être employés par les méthodes cryptographiques dans les couches supérieures de la pile de communication à travers l'implémentation des PUFs.

Références:

[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.