Secure Physical Layer Network Coding based on Homomorphic Cryptography

Host institution : Labortoire LTCI , Telecom ParisTech, 46 rue Barrault, 75013 Paris
Supervisor : Prof. Ghaya Rekaya-Ben Othman, rekaya@telecom-paristech.fr
Duration : 1 year

Stat of the art :

Network Coding [1] has been introduced to enhance the network throughput and improve the system performance. This approach allows to break from the traditional routing paradigm by making intermediate nodes in a communication network allowed to not only forward but also perform processing on the content of the incoming independent data flows. At the network layer, this consists in executing binary operations on the independent bit streams (e.g., bitwise exclusive-OR), while at the physical layer, Network Coding is made at the signal space level and more general linear or non linear combinations can be operated on the independent incoming signals. Physical-Layer Network Coding (PLNC) [2] has been introduced to improve interference management in wireless networks including multiple access channels. PLNC turns the broadcast and superposition properties of the wireless media into boosting characteristics to achieve higher end-to-end transmission rates. Even if Network Coding is based on a very simple idea of mixing independent information flows, it has a large application potential as cooperative communications, distributed storage, caching , network monitoring [3,4].

From a security point of view, Network Coding has both pros and bottlenecks depending on the application and the network scenario. Looking at the security benefits, coding at intermediate nodes can offer a considerable protection against eavesdroppers. As an example, consider the butterfly network and suppose that an eavesdropper manages to wiretap the channel the source and a relay node. If the relay uses the traditional routing, the adversary can obtain the sent bit. However, when applying Network Coding, the eavesdropper, obtains only a sum of received bits from all sources, and so is unable to decode any of the source bits. Then it is clear that Network Coding can allow a secure communication. More discussions about the impact of Network Coding on the security in wireline and wireless networks are addressed respectively in [5] and [6]. Very recently in [7,8] , a combination of a Network Coding scheme and an Homomographic encryption has been proposed, exploiting the combination property of NC.

Theoretically, Homomorphic Encryption allows working on encrypted data without ever decrypting, which is a major improvement allowing users to benefit from internet services while still keeping their data confidential. Such feature can be very useful for the scientific domain (medical analysis, simulations...), the marketing domain (survey studies, statistics...) or any other field which requires high computation and confidentiality. But in practice, this is more complex and difficult to achieve due to efficiency problems. We can distinguish three classes of Homomorphic Encryption depending on the complexity of the operations they allow :

- Partially Homomorphic cryptosystems allow to evaluate elementary operations of only one fixed type, for instance only additions, or only multiplications. Many standard cryptographic primitives (such as the RSA, El Gamal, or Pallier cryptosystems [9,10]) often admit such a partial homomorphic property, coming from their algebraic constructions.

- Somewhat Homomorphic schemes (SHE) allow to evaluate at least two types of operations, for instance both additions and multiplications, or both AND and XOR boolean operations, but only for circuits up to a certain bounded depth. This is due to the introduction of a form of

noise for encryption which grows with the depth of the computation. Although one can imagine applications for which such schemes would be useful. Originally, they have been introduced only as a first step toward Fully Homomorphic Encryption.

- Fully Homomorphic Encryption (FHE) theoretically allow to perform arbitrary computations on the encrypted data. The key point in their construction from SHE is Gentry's bootstrapping technique [11] which serves to control the noise growth. Gentry's original scheme is based on lattices and the Learning with error problem. Other schemes using more elementary tools, such as basic integer arithmetic, have also been proposed [12]. Unfortunately, up to now, all these propositions remain too heavy for practical implementation.

By using PLNC, intermediate nodes decode and forward a function of the original signals without decoding each one of them separately in contrast to straightforward Network Coding which mixes the already decoded bits. So it could be interesting to exploit this property to define an homomographic encrytoion based on lattice coding. We aim to prove through this work that in addition to bandwidth efficiency and robustness improvement of PLCN, it can also be used as an efficient solution to preserve secrecy and privacy in the network.

Research Work

In this work, we will explore coding techniques based on Lattice theory in order to meet secrecy requirement. Lattice Coding is used in several applications like Multiple-Input-Multiple-Output (MIMO) systems, Network Coding, Cryptography and recently for Physical layer secrecy. For example, practical codes were designed to achieve the physical layer secrecy capacity based on classic and modern coding techniques and on structured nested lattice codes in [13,14].

The question of secrecy and privacy of physical layer network coding will be addressed, with the objective to make it fully homomographically crypteted. The matter is that eavesdropper will have no information when accessing network nodes or intercepting message. For that, we will design a compute and forward (CF) scheme [15,16,17] using a multi-layer nested lattice code, where the lattice code will ensure secrecy/privacy and reliable PLCN scheme.

We are interested in PLNC using lattice-based channel coding and homographic encryption. In particular, we propose to design and analyze the performance of the multi-layer nested lattice CF scheme for different multiuser network configurations. For That the research work will be dived into 3 parts :

1. Bibliography study of lattice coding, Physical layer network coding and homomorphic cryptography.
2. Propose an homomorphic encryption based on multi-layer nested lattice for Physical layer network coding.
3. Evaluation of the proposed scheme in terms of transmission efficiency and secrecy.

Initial results of this research work will be submitted to IEEE conferences, and once the initially developed ideas and techniques evolved into significant contributions, we will submit them to international journals of the field, such as IEEE Transactions on different topics. We expect also that parts of the research results would lead to patents, mainly the design of new codes and cryptographic schemes.

Bibliographie

[1] R.W. Yeung, S-Y.R. Li, N.Cai, and Z. Zhang, "Network coding theory". Foundations and Trends in Com. and Inf. Theory, 2005.

[2] S. Zhang, S. Liew and L. Lu. "Physical-layer network coding : Tutorial, survey, and beyond". Elsevier Physical Com. Journal, 2011.

[3] S. K. Dash, S. Mohapatra and P. K. Pattnaik, "A Survey on Applications of Wireless Sensor Network Using Cloud Computing", Int. Journal of Computer Science & Emerging Technologies, vol. 1, no. 4, 2010.

[4] A. Ravi1, P. Ramanathan and K. M. Sivalingam, "Integrated Network Coding and Caching in Information-Centric Networks", IEEE ANTS, 2014.

[5] T. Ho and L. Desmond, "Network Coding : An Introduction", Cambridge University Press, New York, NY, USA, 2008.

[6] J. Dong, R. Curtmola, and R. Sethi et al., "Toward secure network coding in wireless networks : Threats and challenges". In 4th Workshop on Secure Network Protocols, 2008.

[7] S-M Choi and J-S Park,"Performance of Secure Network Coding based on Homomorphic Encryption", IEEE ICUFN, 2016.

[8] Oksana Turshina, "On the Anonymity of Physical-Layer Network Coding against wiretapping", IEEE REDUNDANCY 2016.

[9] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes", In Advances in cryptology—EUROCRYPT'99 (pp. 223-238), Springer Berlin Heidelberg, January 1999.

[10] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", In Advances in Cryptology (pp. 10-18), Springer Berlin Heidelberg, January 1985.

[11] M. Van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, "Fully homomorphic encryption over the integers", In Advances in cryptology–EUROCRYPT(pp. 24-43), Springer Berlin Heidelberg, 2010.

[12] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[13] X. He and A. Yener, "Providing secrecy with structured codes : Tools and applications to Gaussian two- user channels," IEEE Trans. Inf. Theory, VOL. 60, NO. 4, APRIL 2014.

[14] F. Oggier, P. Solé and J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel : Construction and Analysis," IEEE Trans. Inf. Theory, October 2015.

[15] B. Nazer and M. Gastpar, "Compute-and-forward : Harnessing interference with structured codes", ISIT 2008.

[16] A. Mejri, G. Rekaya-Ben Othman and J-C. Belfiore, "Lattice Decoding for the Compute-and-Forward Protocol", ICCN, Tunisia, March 2012.

[17] A. Mejri and G. Rekaya-Ben Othman, "Practical Physical Layer Network Coding in Multi-Sources Relay Channels via the Compute-and-Forward", WCNC, April 2013.