COST Action IC1104

Report on the Activities of Working Group 3

Working Group 3 is concerned with the connections between cryptography and network coding. Topics addressed in this 6 month period include (a) McEliece-style cryptosystems, and their relations with network coding techniques; (b) Gaussian and fading wiretap channels; (c) general physical layer security. This has led to the following new research outputs over the past 6 months.

- M. Baldi, F. Chiaraluce, J. Rosenthal, D. Schipani, “An improved variant of McEliece cryptosystem based on Generalized Reed-Solomon codes”, Proc. Effective Methods in Algebraic Geometry (MEGA 2015), Trento, Italy, 15-19 June 2015. This publication falls under topic (a). The speed and security of such systems, together with their possible quantum-resistance, makes the study of McEliece variants apposite in a network coding context.
- Physical and Data-Link Security Techniques for Future Communication Systems (M. Baldi, S. Tomasin, Eds.), Vol. 358 of Springer Lecture Notes in Electrical Engineering, 2016. This falls under topics (b) and (c). The book is a collection of invited chapters on the theme of securing channels against eavesdroppers using the physical and data-link layers of a channel. This is especially relevant for network coding applications, as the applications’ high data throughput asks for security solutions that are computationally light. Many of the chapters are closely associated with the work carried out under Working Group 3.
- Arsenia Chorti, Camilla Hollanti, Jean-Claude Belfiore, and Vincent Poor, "Physical layer security: a paradigm shift in data confidentiality", Springer Lecture Notes in Electrical Engineering, invited book chapter, 2015. See above. This falls under topics (b) and (c). This work presents advances in the area of physical layer security, and creates a platform for future development.
- Alex Karrila and Camilla Hollanti, "A comparison of skewed and orthogonal lattices in Gaussian wiretap channels", 2015 IEEE Information Theory Workshop (ITW), Jerusalem, Israel, April 2015. This falls under topic (b). Final version of paper referred to in the last report. The performance of orthogonal nested

lattices are analysed when they are used with Gaussian wiretap channels.

- David Karpuk, Anne-Maria Ernvall-Hytöonen, Camilla Hollanti, Emanuele Viterbo, "Probability estimates for fading and wiretap channels from ideal class zeta functions", Advances in Mathematics of Communications, AIMS, Nov. 2015. This falls under topic (b). A journal version of the preprint announced in the last report. New probability estimates are derived for ideal lattice codes from totally real number fields using ideal class Dedekind zeta functions. These results allow an analysis of an adversaries' success in a class of fading wiretap channels.