REPORT ON THE ACTIVITIES OF WORKING GROUP 3

The group has been working on the following topics: (a) McEliece-style cryptosystems based on network coding techniques; (b) strong secrecy in wireless network coding; (c) Gaussian and fading wiretap channels; (d) network coding and stream ciphers.

1 Papers and preprints

[1] Strong Secrecy in Wireless Network Coding Systems with M-QAM Modulators
Arsenia Chorti, Mehdi M. Molu, David Karpuk, Camilla Hollanti, Alister Burr
Appeared in ICCC 2014
http://arxiv.org/abs/1407.0915

[2] Probability Estimates for Fading and Wiretap Channels from Ideal Class Zeta Functions David Karpuk, Anne-Maria Ernvall-Hytnen, Camilla Hollanti, Emanuele Viterbo
Revised version submitted to AMC Dec. 2014
http://arxiv.org/abs/1412.6946

[3] A Comparison of Skewed and Orthogonal Lattices in Gaussian Wiretap Channels
Alex Karrila, Camilla Hollanti
To appear in ITW 2015, April 2015
http://arxiv.org/abs/1411.5861

Paper [1] relates to topic (b). In this paper the authors develop physical layer network coding schemes with embedded strong secrecy based on standard QAM modulators. Their schemes have the potential of increasing data throughput without compromising the confidentiality of the exchanged data in certain security models of wide interest.

Papers [2] and [3] relate to topic (c). In [2], 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. In [3], the performance of orthogonal nested lattices are analysed when they are used with Gaussian wiretap channels.

2 Other activities

The material in [1] has been presented at the 2014 IEEE/CIC International Conference on Communications in China (ICCC).

Joachim Rosenthal and Kyle Marshall have studied the security of McEliece-type cryptosystems where Gabidulin codes (which underpin network coding techniques) are used rather than the traditional error correcting codes proposed by McEliece and others. This falls under topic (a). A new attack, based on geometric ideas, is constructed which is capable of breaking several variants of such cryptosystems that have been proposed in the literature. Many of the results were presented at ALCOMA 15, in the talk McEliece type Cryptosystems based on Gabidulin Codes (by Joachim Rosenthal), and a publication is planned.

Tor Helleseth and Sondre Rnjom have been investigating network coding as applied to stream ciphers. Their work was mentioned in Tor Helleseth's plenary lecture in ALCOMA 15; publication is planned.