List of Publications

PhD Thesis

2017 **An algebraic approach for the resolution of algorithmic problems raised by cryptography and coding theory**

https://tel.archives-ouvertes.fr/tel-01690012/file/dragoivladflorin2.pdf

International Conferences

2018 **Vulnerabilities of the McEliece Variants Based on Polar Codes**, *Vlad Drăgoi, Valeriu Beiu, Dominic Bucerzan*, International Conference on Security for Information Technology and Communications (SecITC), November 8–9, 2018, Bucharest, Romania. (Scopus).

https://link.springer.com/chapter/10.1007/978-3-030-12942-2_29

2018 **Effective Conductances of Moore-Shannon Hammocks**, *Simon R. Cowell, Vlad Dragoi, Valeriu Beiu, Noemi Rohatinovici*, IEEE International Conference on Nanotechnology (IEEE-NANO), Cork, Ireland, JUL 23-26, 2018 (ISI WOS).

http://dx.doi.org/10.1109/NANO.2018.8626295

2018 **Ordering Series and Parallel Compositions**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu*, IEEE International Conference on Nanotechnology (IEEE-NANO), Cork, Ireland, JUL 23-26, 2018 (ISI WOS).

http://dx.doi.org/10.1109/NANO.2018.8626408

2018 **Survey on Cryptanalysis of Code-Based Cryptography : From Theoretical to Physical Attacks**, *Vlad Dragoi, Tania Richmond, Dominic Bucerzan and Axel Legay*, IEEE International Conference on Computers Communications and Control, Baile Felix, Oradea, Romania, May 2018. (ISI WOS, Scopus).

http://dx.doi.org/10.1109/ICCCC.2018.8390461

2018 **Hammocks versus Hammock**, *Valeriu Beiu, Simon R. Cowell, Vlad Dragoi, Sorin Hoară and Păstorel Gașpar*, IEEE International Conference on Computers Communications and Control, Baile Felix, Oradea, Romania, May 2018. (ISI WOS, Scopus).

http://dx.doi.org/10.1109/ICCCC.2018.8390447

2018 **Can Series and Parallel Compositions Improve on Hammocks ?**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gașpar*, IEEE International Conference on Computers Communications and Control,Baile Felix, Oradea, Romania, May 2018. (ISI WOS, Scopus).

http://dx.doi.org/10.1109/ICCCC.2018.8390448

2018 **On Algorithms for Evaluating the Reliability of Large Hammock Networks**, *Noemi-Clara Rohatinovici, Valeriu Beiu, Simon R. Cowell, Leonard Daus, Vlad Dragoi and Valentina Emilia Balas*, IEEE International Conference on Computers Communications and Control,Baile Felix, Oradea, Romania, May 2018. (ISI WOS, Scopus).

http://dx.doi.org/10.1109/ICCCC.2018.8390449

2017 **The Simple Roots Problem**, *Dominic Bucerzan, Vlad Dragoi and Tania Richmond*, Romanian Cryptology Days (RCD), Sept. 18-20, 2017, Bucharest, Romania. (ISI WOS, Scopus).

http://www.acad.ro/sectii2002/proceedings/doc2017-4s/03artSupl.pdf

2017 **Evolution of the McEliece Public Key Encryption Scheme**, *Dominic Bucerzan, Vlad Dragoi and Hervé Talé Kalachi*, International Conference on Security for Information Technology and Communications (SecITC), June 8-9, 2017, Bucharest, Romania. (Scopus).

https://link.springer.com/chapter/10.1007/978-3-319-69284-5_10

2016 **Algebraic Properties of Polar Codes From a New Polynomial Formalism**, *Magali Bardet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, IEEE International Symposium on Information Theory (ISIT), July 10-15, 2016, Barcelona, Spain. (ISI WOS, Scopus).

`http://dx.doi.org/10.1109/ISIT.2016.7541295`

2016 **Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme**, *Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, Ayoub Otmani*, Progress in Cryptology – AFRICACRYPT, April 13-15, 2016, Fes, Morocco. (Scopus).

`http://dx.doi.org/10.1007/978-3-319-31517-1_18`

2016 **Cryptanalysis of the McEliece Public Key Cryptosystem based on Polar Codes**, *Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, International Workshop on Post Quantum Cryptography (PQCrypt), Feb. 24-26, 2016, Fukuoka, Japan. (ISI WOS, Scopus).

`http://dx.doi.org/10.1007/978-3-319-29360-8_9`

2015 **Etude d'un Système de Chiffrement de Type McEliece à Base de Codes Polaires**, *Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, Jean-Pierre Tillich*, Journées Codage et Cryptographie, La Londe-les-Maures, Franța.

`https://hal.inria.fr/hal-01240843/`

2013 **Polynomial Structures in Code-based Cryptography**, *Vlad Dragoi, Pierre-Louis Cayrel, Brice Colombier, Tania Richmond*, 14th International Conference on Cryptology in India, Dec. 7-10, 2013, Mumbai, India. (Scopus).

`http://dx.doi.org/10.1007/978-3-319-03515-4_19`

International Journals

2019 **Studying the binary erasure polarization subchannels using network reliability**, *Vlad Drăgoi, Valeriu Beiu*, IEEE Communications Letters, in press, 2019. (ISI WOS, Scopus).

`http://doi.org/10.1109/LCOMM.2019.2947910`

2018 **How Reliable are Compositions of Series and Parallel Networks Compared with Hammocks ?**, *Vlad Dragoi, Simon R. Cowell, Valeriu Beiu, Sorin Hoară and Păstorel Gașpar*, International Journal of Computers Communications & Control, vol. 13, no. 5, 2018. (ISI WOS, Scopus).

`https://doi.org/10.15837/ijccc.2018.5.3354`

2018 **Cryptanalysis of a Public Key Encryption Scheme Based on QC-LDPC and QC-MDPC**, *Vlad Dragoi, Hervé Talé Kalachi* , IEEE Communications Letters, vol. 22 ,pp. 264-267, Feb. 2018. (ISI WOS, Scopus).

`http://doi.org/10.1109/LCOMM.2017.2779449`

2017 **Improved Timing Attacks against the Secret Permutation in the McEliece PKC**, *Dominic Bucerzan, Pierre-Louis Cayrel, Vlad Dragoi, Tania Richmond*, International Journal of Computers Communications & Control , vol. 12, no. 1, pp. 7-25, 2017. (ISI WOS, Scopus).

`http://dx.doi.org/10.15837/ijccc.2017.1.2780`

Accepted Abstracts

2018 **The posets for reliability : How fine can they be ?**, *Valeriu Beiu, Simon R. Cowell, Vlad Dragoi*, SOFA 2018.