Algebraic approach in code-based cryptography

McEliece's encryption scheme represents one of the solutions to the security issues that are raised by the possible arrival of quantum computers. The main objective in this presentation is to analyze the security of the McEliece variants based on MDPC and polar codes.

In the case of the MDPC based variant, we reveal a subset of private keys that present an important weakness. We propose an efficient algorithm that retrieves, for the set of weak keys, the private key given the public data. Next, we count the proportion of weak keys and we use the code equivalence problem to extend the number of keys, that can be retrieved with the aforementioned algorithm.

We next study the polar codes and their application to public key cryptography. From an information theory point of view, polar codes have been one of the most studied families of codes, ever since their discovery by Arikan. They are extremely efficient in terms of performance as they are capacity achieving over the Binary Discrete Memoryless Channels and they allow extremely fast encoding and decoding algorithms. However, only a few facts are known about their structure. In this context, we introduce an algebraic formalism which allows us to reveal a big part of their structure. We exhibit a few fundamental traits of polar codes: the dual, the minimum distance, the permutation group and the number of minimum weight codewords.

We also completely cryptanalyze the McEliece variant using polar codes. The attack is a direct application of the later results on the structure of polar codes.

Vlad F. Dragoi was born in Arad, Romania in 1984. He received the B.Sc. degree in mathematics and the M.Sc. degree in applied mathematics, both from the Claude Bernard University Lyon 1, Lyon, France, in 2011 and respectively 2013, and the Ph.D. degree in computer science from the University of Rouen Normandy, Rouen, France, in 2017.

Since 2018, he is a Research Fellow (postdoctoral level) with the "Aurel Vlaicu" University of Arad (UAV), Arad, Romania, where he has also started to lecture part-time. He has published 17 journal/conference articles, and gave 12 talks to international conferences/workshops. His research interests include post-quantum cryptography (focusing on code-based cryptography), discrete mathematics applied in error correcting codes, and network reliability.

Dr. Dragoi received an Agence Nationale de la Recherche (ANR) doctoral scholarship from 2013 to 2016, and is the recipient of two IEEE best paper awards.