Code based cryptography: current challenges.

Leen Demuys

Vrije Universiteit Brussel

Code based cryptography relies on the hardness of decoding a random linear code. In this talk, we will focus on the use of linear codes for developing public key cryptosystems. The first such cryptosystem was proposed by Robert McEliece in 1978. Recently, an adaptation of this scheme was selected by NIST as finalist in a competition to establish post-quantum cryptography standards for public-key cryptography.

While McEliece's original scheme makes use of Goppa codes, it is uncertain whether this is the most secure or efficient approach. This prompts the investigation of alternative codes with desirable properties, such as smaller key length, or higher error correction capacity. We will discuss McEliece's original method, as well as more recent developments in this field. We will conclude with stating some open questions which we intend to pursue in future research.

Vrije Universiteit Brussel, Department of Mathematics and Data Science Pleinlaan 2, 1050 Elsene, Belgium
Leen.Demuys@vub.be