1163-15-1666 **Ray A Perlner*** (ray.perlner@nist.gov). *MinRank and its Application to Cryptanalysis.*

The MinRank problem is an important problem in multivariate and code-based cryptography, representing a major avenue for attacks against several encryption and signature schemes, including the third round candidates in the NIST PQC standardization process, Rainbow and GeMSS, as well as the second round candidates ROLLO and RQC. It involves finding a low rank linear combination of a collection of matrices over a finite field. In most cases the instance of MinRank involved in key recovery has additional structure, which may or may not be exploitable by the attacker. Various algebraic and combinatorial approaches have been explored for solving the problem. This talk will focus on joint work with Bardet, Bros, Cabarcas, Gaborit, Smith-Tone, Tillich, and Verbel appearing at Asiacrypt 2020, which resulted in a major change in the estimated security of the schemes ROLLO and RQC and a major change in the estimated complexity of MinRank attacks against Rainbow and GeMSS. (Received September 16, 2020)