1161-14-221 **Daniel C Smith-Tone*** (daniel-c.smith@louisville.edu). *Algebraic Models for the MinRank Problem and How Dramatically Our World is Changing.*

The MinRank Problem is a natural complexity theoretic problem closely related to cryptanalytic attacks on code- and multivariate-based schemes. Various methods of modelling the computational version of this problem exist, including two historically dominant algebraic techniques. For over a decade the so-called minors method has been supposedly proven to be superior to the Kipnis-Shamir (KS) method and any other method by way of a simple but trivially false argument.

We demonstrate the fallacy of the above claim by providing a tight analysis of the KS method in "superdetermined" MinRank instances as well as by introducing a new algebraic model that dramatically reduces the complexity of MinRank over a large parameter space. We then discuss the rather dramatic impact this new technique has on post-quantum cryptography. (Received August 17, 2020)