1161-14-274 **Jintai Ding**, **Joshua Deaton*** (deatonju@mail.uc.edu), **Vishakha** and **Bo-Yin Yang**. *The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV which Forges a Signature within 210 Minutes.*

In 2017, Ward Beullens et al. submitted Lifted Unbalanced Oil and Vinegar, which is a modification to the Unbalanced Oil and Vinegar Scheme by Patarin. Previously, Ding et al. proposed the Subfield Differential Attack which prompted a change of parameters by the authors of LUOV for the second round of the NIST post-quantum standardization competition. We have developed a refinement to the Subfield Differential Attack called the Nested Subset Differential Attack which fully breaks half of the parameter sets put forward. We also show by experimentation that this attack is practically possible to do in under 210 minutes for the level I security parameters and not just a theoretical attack. The Nested Subset Differential attack is a large improvement of the Subfield differential attack which can be used in real-world circumstances. Moreover, we will only use what is called the "lifted" structure of LUOV, and our attack can be thought of as a development of solving "lifted" quadratic systems. (Received August 18, 2020)