1157-15-506 **Angela Robinson***, angela.robinson@nist.gov. *Attacking product structure of LEDAcrypt.*

The 2nd Round submission to NIST's Post Quantum Cryptography standardization process, LEDAcrypt, is based on quasi-cyclic low-density parity check codes. The public parity check matrix of the code in systematic form is generated by taking a product of two sparser matrices with quasi-cyclic structure. We present an attack that exploits the product structure of LEDAcrypt's key in a non-trivial manner by using information set decoding on structured information sets. We believe that in all parameter sets proposed in the LEDAcrypt submission, there are substantial classes of weak keys that can be recovered significantly faster than would be expected from the usual analysis, and in some cases, ithe security level of the average key is also weaker than expected. (Received February 03, 2020)