1163-06-1236 **Shuhong Gao**, **Ryann Cartor*** (rcartor@clemson.edu), **Benjamin Case**, **Yan Ren** and **Hui Xue**. *Lattice-based Signature Scheme based on M-SIS.*

The 3rd round candidates of the NIST post-quantum cryptography include two signature schemes based on lattices, namely Falcon and Dilithium. Falcon is based on NTRU and has much smaller signature sizes, while Dilithium is based on M-RLWE and is fast and easy to implement. The current paper presents a signature scheme based on M-RLWE and has smaller signature size than Dilithium's under the same security levels. The new signature scheme has signature sizes only slightly bigger than Falcon's but does not require expensive Gaussian sampling. (Received September 15, 2020)