**Abstract:**

This paper presents MQDSS, the first signature scheme with a security reduction based on the problem of solving a multivariate system of quadratic equations (MQ problem). In order to construct this scheme we give a new security reduction for the Fiat-Shamir transform from a large class of 5-pass identification schemes and show that a previous attempt from the literature to obtain such a proof does not achieve the desired goal. We give concrete parameters for MQDSS and provide a detailed security analysis showing that the resulting instantiation MQDSS-31-64 achieves 128 bits of post-quantum security. Finally, we describe an optimized implementation of MQDSS-31-64 for recent Intel processors with full protection against timing attacks and report benchmarks of this implementation.

**Keywords:** post-quantum cryptography, Fiat-Shamir, 5-pass identification scheme, vectorized implementation.