From: javier verbel <javh10@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Concrete hardness estimates of the MQ problem
Date: Wednesday, August 03, 2022 05:17:12 AM ET

Hello everyone,

We are happy to share with you the MQ-estimator (https://github.com/Crypto-TII/multivariate_quadratic_estimator). This is a sage package to estimate the hardness of solving Multivariate Quadratic (MQ) problem, which is related to the security of multivariate-public key cryptosystems (MPKC). A preprint accompanying sage package is available at https://eprint.iacr.org/2022/708.pdf.

In addition to the complexity estimator, our sage package also provides modules to construct toy instances of several MPKC schemes such as UOV, Rainbow, and GeMSS. These modules will be useful for experimental and educational purposes.
The project's vision is to provide to the cryptographic community a common tool to precisely estimate the security of Multivariate-based cryptosystems.

We are open to contributions and future discussions.

Best Regards,
Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, Javier Verbel