From: 'Edoardo Persichetti' via pqc-forum <pqc-forum@list.nist.gov>
Sent: Friday, July 21, 2023 11:44 AM
To: pqc-forum
Subject: [pqc-forum] OFFICIAL COMMENT: LESS

Dear all

With the present email, the LESS team would like to point out that the technique used to attack ALTEQ, and MEDS, can be used in the LESS setting as well. Indeed, we have confirmed with Tung Chou that a modified version of the attack applies; similarly to the other schemes, the scheme is vulnerable if the transmitted matrices are not properly formed. In our case, this means that the algorithm should explicitly check that the matrices are indeed monomial (thus have exactly one non-zero value in each row and column). This is not currently enforced in the specification document. Note that the cost of the attack is non-trivial, and the attack does not work for the setting s=2; however, enforcing such a check on the monomial matrices is enough to fully avoid it in the first place.

We will proceed to modify both the specification document, and the implementation as quickly as possible; the updated versions will be available on our website http://www.less-project.com/. The proposed modifications do not affect the signing process, or interoperability with the submitted version. The same KAT test vectors can be used.

We would like to thank the community for your interest, and extensive scrutiny of our submission!

Best,
Edoardo (on behalf of the LESS team)
--