Dear Markku, Ward, and all,

We confirm that a variant of the attack (details see below) described by Markku-Juhani O. Saarinen and Ward Beullens in previous threads commenting on ALTEQ also applies to MEDS, which for example reduces the attack success probability on the Fiat-Shamir construction for the Level-I parameter sets to $2^{-89.1}$ and $2^{-105.9}$.

We concur that checking if the signature matrices are invertible during verification invalidates the attack.

We will update the specification document and the source code accordingly and we will make both available on the MEDS website: [https://www.meds-pqc.org/](https://www.meds-pqc.org/)

Thanks to the whole community for the thorough scrutiny and the constructive feedback!

Best regards

MEDS team

Attack variant:

The attack as previously described by Markku and Ward does not straightforwardly match to MEDS, since we are checking during verification if the resulting matrix has systematic form, which is not the case if the signature matrices $\mu_i$ and $\nu_i$ are zero.

However, Ward Beullens pointed out to us that the resulting matrix can easily be forced to be the identity matrix in the left and all zeros in the right after systemization by setting one of the signature matrices to any invertible matrix and the other to a non-zero first row and all-zero in the remaining rows. Then, the $\pi()$ operation results in an invertible matrix in the left and all zero in the right - and the following systemization results in the desired shape.
Dear all,

As announced in our previous email, we have updated our spec and implementation to fix our multi-key Fiat-Shamir construction.

We also took the opportunity to improve the multi-target collision resistance of MEDS.

The updated submission document and the source code can be found on our website: https://www.meds-pqc.org/

and via the following links:

- Submission document:

- Reference implementation:

https://github.com/MEDSpqc/meds

- KAT files:

Best regards
MEDS team