From: Ruben Niederhagen <ruben@polycephaly.org>
Sent: Wednesday, July 19, 2023 9:51 PM
To: pqc-comments
Cc: pqc-forum; author-contact@meds-pqc.org
Subject: Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS

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/

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 straight forwardly 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.

From: Ruben Niederhagen <ruben@polycephaly.org>
Sent: Wednesday, July 26, 2023 5:18 AM
To: pqc-comments
Cc: pqc-forum; author-contact@meds-pqc.org
Subject: Re: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS

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:
https://www.meds-pqc.org/spec/MEDS-2023-07-26.pdf

- Reference implementation:
https://www.meds-pqc.org/pack/MEDS-2023-07-26.tgz

https://github.com/MEDSpqc/meds

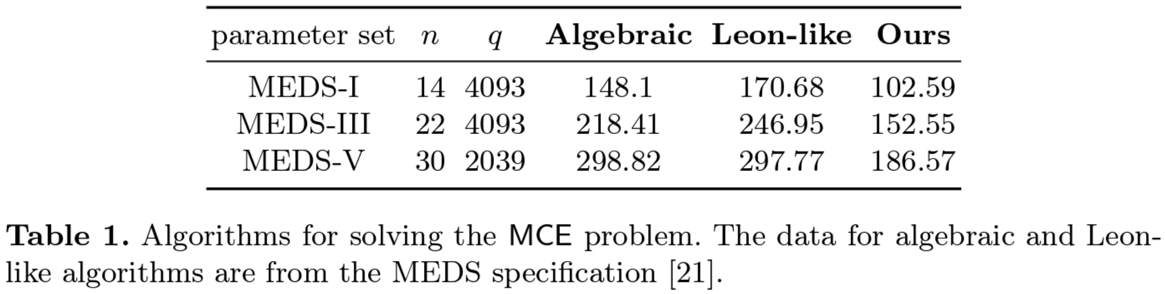
- KAT files:
https://www.meds-pqc.org/KAT/MEDS-KAT-2023-07-26.tgz

Best regards
MEDS team

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> **On Behalf Of** Youming Qiao
Sent: Thursday, March 7, 2024 4:54 AM
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS

Dear all,

We would like to report that we devise a new algorithm for matrix code equivalence, available at https://eprint.iacr.org/2024/368. This algorithm then has the following implication to MEDS parameters (table taken from the paper):



parameter set	n	q	**Algebraic**	**Leon-like**	**Ours**
MEDS-I	14	4093	148.1	170.68	102.59
MEDS-III	22	4093	218.41	246.95	152.55
MEDS-V	30	2039	298.82	297.77	186.57

Table 1. Algorithms for solving the MCE problem. The data for algebraic and Leon-like algorithms are from the MEDS specification [21].

We have timely communicated this with the MEDS team.

Best regards,
Anand Kumar Narayanan, Youming Qiao, and Gang Tang

From: pqc-forum@list.nist.gov on behalf of simona s <simona.samardziska@gmail.com>
Sent: Wednesday, March 13, 2024 11:38 AM
To: Youming Qiao
Cc: pqc-forum
Subject: Re: [pqc-forum] Round 1 (Additional Signatures) OFFICIAL COMMENT: MEDS

Dear all,

The MEDS team would like to thank Anand, Youming and Gang for showing interest in our scheme MEDS and the clever observation leading to reducing the security level of the Round 1 MEDS parameters.
We acknowledge that the new non-trivial invariant found by them indeed exists for the matrix codes used in MEDS. In order to be secure against this attack we need to increase the parameters of MEDS. We will soon publish the updated parameters.

Note that using a new optimization technique that we have developed for MEDS, even with the required increase of parameters due to the above algorithm, we can still maintain and even improve upon the signature sizes of our current set of parameters for all three security levels. Our optimization technique which was sketched in Section 8 of our specs will soon be made public.

All the best,
The MEDS team

On Thu, Mar 7, 2024 at 10:54 AM Youming Qiao <jimmyqiao86@gmail.com> wrote:

> Dear all,
>
> We would like to report that we devise a new algorithm for matrix code equivalence, available at https://eprint.iacr.org/2024/368. This algorithm then has the following implication to MEDS parameters (table taken from the paper):