From: simona s <simona.samardziska@gmail.com>
Sent: Monday, September 03, 2018 8:11 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: MQDSS

Dear all,

Recently, after a related inquiry by Eliane Koussa and Ludovic Perret, we noticed that we have made a mistake in the choice of parameters in the NIST submission of MQDSS. In particular, the number of rounds in the submission is twice bigger than it is actually needed for the respective security level. This means that the number of rounds can be halved without affecting the security of the scheme, while substantially improving its performance:
the signing and verification time will be halved, and (even more importantly,) the signature size will be halved.

We therefore announce a new Version 1.1 of MQDSS, in which this mistake has been corrected.
The specification and implementation of MQDSS Version 1.1. are available through our (brand new) web site http://mqdss.org
(Direct link to specification: http://mqdss.org/files/MQDSS_Ver1point1.pdf
and to reference implementation https://github.com/joostrijneveld/MQDSS/tree/NIST)

The new parameters of MQDSS give the following performance results:

	Public key (bytes)	Secret key (bytes)	Signature (KiB)
MQDSS-31-48	46	16	16.15
MQDSS-31-64	64	24	33.23

Reference implementation:

	keygen (cycles)	signing (cycles)	verification (cycles)
MQDSS-31-48	1302K	26500K	19674K
MQDSS-31-64	2769K	84615K	63210K

Implementation using AVX2 instructions:

	keygen (cycles)	signing (cycles)	verification (cycles)
MQDSS-31-48	1078K	3683K	2504K
MQDSS-31-64	2495K	8709K	6183K

We respectively hope that NIST will take into account the new parameters of MQDSS for the first round of the PQC standardization process, especially since they only improve the performance of the scheme (the security remains the same).
We also understand that NIST has the right to evaluate the candidates based solely on the initial submission.

Sincerely,
The MQDSS team