From: Kirk Fleming <kpfleming@mail.com>
Sent: Monday, November 9, 2020 8:35 PM
To: pqc-comments
Cc: pqc-forum
Subject: ROUND 3 OFFICIAL COMMENT: Classic McEliece

There is a strong possibility that NIST intend to standardize Classic McEliece at the end of Round 3 as a conservative option. Their Status Report on the Second Round expressed confidence in its construction and said that they believed it could be ready for standardization if selected. Standardizing Classic McEliece, however, also means standardizing at least some of the parameter sets proposed by the submitters.

I am filing this comment to request that the Classic McEliece submitters justify the claimed security categories for their parameters.

The Round 3 submission does not include any concrete analysis of the security provided by the proposed parameter sets. There is a lot of hype about the asymptotic result from Canto Torres and Sendrier but this is ultimately irrelevant for any finite choice of parameters. The only firm statement contained in the submission is:

> "[Bernstein, Lange and Peters. 2008] reported that its attack uses 2^266.94 bit operations to break the (13,6960,119) parameter set. Subsequent ISD variants have reduced the number of bit operations considerably below 2^256."

The submission argues that any reduction in classical security from improved ISD attacks will be offset by the increased memory requirements. While this may be true for some ISD variants such as BJMM, they provide no analysis to back this up. It also ignores other ISD variants such as Stern that need significantly less memory. In this case the finite regime analsysis from the LEDACrypt team gives the following estimates of computational and memory costs for the pre-merger Classic McEliece and NTS-KEM parameters:

Parameter Set	Compute	Memory	Target
mceliece-3488-064	152.51	34.68	143
mceliece-4608-096	194.36	35.66	207
mceliece-6688-128	270.46	37.48	272
mceliece-6960-119	271.18	47.58	272
mceliece-8192-128	306.63	67.64	272
nts-kem-4096-064	166.76	35.60	143
nts-kem-8192-080	248.01	77.63	207
nts-kem-8192-136	313.52	67.50	272

By this analysis:

- The mceliece-4608-096 parameters are about 13 bits below Category 3 with an attack that needs slightly over 6 GiB of memory.

- The mceliece-6688-128 parameters are borderline Category 5 with an attack that needs slightly over 22 GiB of memory.

- The mceliece-6960-119 parameters are borderline Category 5 with an attack that needs around 24 TiB of memory.

If Classic McEliece is to be standardized as a conservative option then the parameter sets that are standardized with it should also be chosen conservatively. The NTS-KEM parameters were. Three out of the five Classic McEliece parameters were not.

Kirk

From: Kirk Fleming <kpfleming@mail.com>
Sent: Wednesday, November 11, 2020 12:20 PM
To: pqc-forum
Cc: pqc-comments
Subject: Re: [pqc-forum] ROUND 3 OFFICIAL COMMENT: Classic McEliece

Kirk Fleming wrote:
> In this case the finite regime analysis from the LEDACrypt team gives the following
> estimates of computational and memory costs for the pre-merger Classic McEliece
> and NTS-KEM parameters:

It was pointed out that my finite regime analysis reference was unclear. The figures were taken from Tables 4 and 5 in Baldi, Barenghu, Chiaraluce, Pelosi and Santini, "A finite regime analysis of Information Set Decoding algorithms", Algorithms 12, no. 10 (2019). The paper can be found at https://www.mdpi.com/1999-4893/12/10/209/pdf.

Kirk