From: Apon, Daniel C. (Fed)
To: Perlner, Ray A. (Fed); Kelsey, John M. (Fed); internal-pqc
Subject: Re: Classic McEliece security
Date: Tuesday, October 5, 2021 9:34:22 PM

Agree; in many ways, we're crossing the/a finish line. Let the horses be placed where they came in. =)

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Tuesday, October 5, 2021 7:09 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Classic McEliece security

No. The existing parameter sets are the ones that have been vetted by the community. It's much better to use an existing parameter set and relabel it according to the security we think it has than to ask them to create a new parameter set at the last minute. If we standardize CM and our users are unsatisfied with category 2 security, they can use the category 5 parameters.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Tuesday, October 5, 2021 5:04 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Classic McEliece security

Would we want to ask the CM team for revised parameters? Or for a defense of why their scheme meets level 3 somehow?

--John

From: "Perlner, Ray A. (Fed)" <ray.perlner@nist.gov>
Date: Tuesday, October 5, 2021 at 17:01
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Classic McEliece security

In more detail:

I think this is the latest estimate from the community of the costs of attacking CM: https://eprint.iacr.org/2021/1243.pdf . If we assume the numbers there are accurate, then CM's claimed category 3 parameters don't meet category 3 for any memory cost model (they didn't evaluate Dan's favored sqrt(M)/2^5 cost model, but given how small the memory is in the last line of table 2, that assumption will not bring the parameters up to category 3.) However, I think we can conclude from table 5 that the parameters in question meet category 2. There are also a couple of category 5 parameter sets that could plausibly be downgraded to category 4 if we assume memory access is very cheap, but I'm willing to give CM the benefit of the doubt on those two parameter sets. It looks like all the other schemes meet their security targets. Note that an earlier paper

https://www.researchgate.net/publication/336203573_A_Finite_Regime_Analysis_of_Information_Set_Decoding_Algorithms gave surprisingly low estimates for the cost of the MMT algorithm, which if correct would suggest all of the code-based crypto parameter sets fail to meet their security targets, but according to appendix A of the new paper, this low cost estimate for MMT was in error.

So in summary, assuming https://eprint.iacr.org/2021/1243.pdf is correct:

1. Classic McEliece's "category 3" parameter set cannot be plausibly justified as meeting a security strength category higher than 2 and any CM standard we put out should reflect that.
2. Two of CM's 3 "category 5" parameter sets could be defensibly downgraded to category 4, although it may not be necessary to do so.
3. All the other code-based crypto parameter sets seem fine WRT security against single-target ISD attacks.

From: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
Sent: Tuesday, October 5, 2021 4:28 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Classic McEliece security

I think the answer is pretty definitively no. If we standardize CM, we should probably label that parameter set as category 2.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Tuesday, October 5, 2021 3:55 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Classic McEliece security

Everyone,

Has the question of whether the level 3 version of classic McEliece reaches its claimed security level ever been resolved? My impression is that it has not, though I may have missed something. (My impression is that Dan blew some smoke at the question and pounded on the table a bit but didn't answer, but again, maybe I missed something.).