From: Cooper, David A. (Fed)
To: Perlner, Ray A. (Fed)
Cc: internal-pqc
Subject: Re: Draft message to Classic McEliece: Request for explicit concrete security claims
Date: Tuesday, August 17, 2021 3:53:01 PM

Hi Ray,

I think the second paragraph should be more explicit about what we need. For example:

> Please, at a minimum, provide your concrete estimate for the gate count of the best known attacks against each of the submitted Classic McEliece parameter sets in the Classical RAM model. In cases in which the cost of the attack in the RAM model is too low for the targeted security category, please provide information about the memory requirements for these attacks (e.g., an estimate of the amount of memory required and the number of random accesses to the memory that would be performed). You may also include your estimates for the concrete cost of the best known attacks in any other model of computation you deem relevant.

I also wonder if we should be more specific about the attacks that should be considered. The official submission only references https://eprint.iacr.org/2008/318. It simply dismisses other attacks as irrelevant since they require more memory than https://eprint.iacr.org/2008/318. While the paper that Tanja referenced in her presentation (https://www.mdpi.com/1999-4893/12/10/209/pdf) seems to suggest that MMT would be the least expensive, Elena's response in https://crypto.stackexchange.com/questions/92074/number-of-bit-operations-required-for-information-set-decoding-attacks-on-code-b suggests that BJMM Depth 3 would be least expensive.

Perhaps Elena is incorrect, but it seems that the Classic McEliece team should respond to it.

Thanks,

David

On 8/17/21 12:26 PM, Perlner, Ray A. (Fed) wrote:

> Dear Classic McEliece team
>
> Given recent forum discussion concerning the concrete security of Classic McEliece's parameter sets, we feel it would be helpful if the team would provide official estimates for the concrete security of its parameter sets. It seems the estimates provided thus far have either been incomplete (not assessing all the parameter sets, or sometimes analyzing parameter sets that are somewhat different from what was submitted,) or have disputed accuracy (e.g. a paper cited by the McEliece team for security estimates, would contradict Classic McEliece's security claims, unless it is dramatically underestimating the cost of the MMT algorithm. – our impression is the paper probably is underestimating the cost of MMT, but we would like an official statement from the Classic McEliece regarding which of the security estimates in papers it cites are accurate.)

Please, at a minimum, provide your concrete estimate for the gate count of the best known attack against each of the submitted Classic McEliece parameter sets in the Classical RAM model. You may also include your estimates for the memory requirements for these attacks as well as for the concrete cost of the best known attacks in any other model of computation you deem relevant.

Thanks
NIST-PQC team.