Comment

Seidl, Jan (CZ - Prague) <jaseidl@deloittece.com>

Thu 9/15/2016 12:42 PM

PQC Public Comments

To: pqc-comments <pqc-comments@nist.gov>;

Dear NIST,

I have one suggestion for the Proposed Requirements and Evalutation Cruteria (DRAFT).

Section 2.B.1, paragraph 3:
"For algorithms that have tunable parameters (such as the dimension of some underlying vector space, or the number of equations and variables), the submission document shall specify concrete values for these parameters. If possible, the submission should specify several parameter sets that allow the selection of a range of possible security/performance tradeoffs. In addition, the submitter should provide an analysis of how the security and performance of the algorithms depend on these parameters."

Suggestion:
" For algorithms that have tunable parameters (such as the dimension of some underlying vector space, or the number of equations and variables), the submission document shall specify concrete values for these parameters and the submitter is required to provide an analysis of how the security and performance of the algorithms depend on these parameters. If possible, the submission should specify several parameter sets that allow the selection of a range of possible security/performance tradeoffs.

Thank you.

Best regards,

Seidl Jan