Two Suggestions

Danilo Gligoroski <danilog@item.ntnu.no>

Sat 9/3/2016 6:29 AM

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

Dear NIST,

I have the following two suggestions.

1. For the part "Algorithm Specifications And Supporting Documentation".

In Section 2.B.1. paragraph 3 the current text is:
"To facilitate the analysis of these algorithms by the cryptographic community, submitters are encouraged to also specify parameter sets that provide lower security levels, and to provide concrete examples that demonstrate how certain parameter settings affect the feasibility of known cryptanalytic attacks."

I suggest this sentence to be moved as a separate section that states the following:

"To facilitate the analysis of the submitted algorithms by the cryptographic community, submitters are required to specify parameter sets that provide lower security levels, and to provide concrete examples that demonstrate how certain parameter settings affect the feasibility of known cryptanalytic attacks."

2. Then in connection with this change, in the part "Proposed Evaluation Process" in Section 5.A the paragraph
"When evaluating algorithms, NIST will make every effort to obtain public input and will encourage the review of the submitted algorithms by outside organizations; however, the final decision as to which (if any) algorithm(s) will be selected for standardization is the responsibility of NIST."

to be changed to the following paragraph

"When evaluating algorithms, NIST will make every effort to obtain public input and will encourage the review of the submitted algorithms by outside organizations; NIST encourages the reviewers to demonstrate their findings and attacks both on the versions with parameters that achieve full security levels, as well as on the provided parameter sets with lower security levels; however, the final decision as to which (if any) algorithm(s) will be selected for standardization is the responsibility of NIST."

Rationale for these suggestions:
NIST crypto competitions are highly respected events in the cryptographic and information security community. It is a prestige to participate in the competition and to publish attacks on the proposed algorithms. In the heat of the debates and the competition, there will be a lot of overrated attacks that actually are not so efficient as the attackers would claim. I am proposing the above changes in order to protect the dignity of both the submitters and the attackers and to save a precious time and efforts by the NIST employees and the whole crypto community. If in the submission documentation there are obligatory test parameters that have very low security margin, any published attack on the schemes is encouraged to be demonstrated *practically* on those low level parameters. That will be seen as a correct and honest attempt to analyze the scheme, not just as a malicious attempt to discredit the attacked algorithm.

Best regards,
Danilo!