Re: [Pqc-forum] Comment on Post-Quantum Cryptography Requirements and Evaluation Criteria

alan szepieniec <alan.szepieniec@gmail.com>

Fri 9/16/2016 7:43 AM

PQC Public Comments

To: Danilo Gligoroski <danilog@item.ntnu.no>;

Cc: pqc-comments <pqc-comments@nist.gov>; pqc-forum <pqc-forum@nist.gov>;

Hi all, hi Danilo,

I like this suggestion, but at the same time I think it is as likely to lead to good outcomes as bad ones. The security of cryptosystems tends to rely not on one difficult problem but rather on a chain of difficult problems in which any one weak link can be enough to break the system. Requiring submitters to provide parameters associated with lower security levels amounts to requiring them to weaken at least one link, while not providing any incentives to weaken the other links as well. Any successful weak-parameter attack shows only that that one link is weak; it offers no indication of the strength of the rest of the chain.

Sorry to be so metaphorical. Here is an example. Suppose you were to propose a signature scheme whose security relies on a) the difficulty of finding inverse images under a function F; and b) the difficulty of finding collisions of function G. Then you could propose weak parameter sets that would make finding collisions for G doable in 2^40 steps and finding inverse images under F only doable in 2^128 steps or more. This course of action is tempting especially if you're more confident in the security estimate of G than of F. Cryptanalytic efforts would be focused on G and not on F, even though for the given weak parameter set F might only offer 2^90 bits of security and not 2^128. Attacks breaking the signature scheme in 2^40 steps validate the security estimate of G but not of F.

best regards,
Alan

On Sat, Sep 3, 2016 at 4:10 PM, Danilo Gligoroski <danilog@item.ntnu.no> wrote:
> Dear NIST,
>
> I have the following two suggestions for the draft requirements and evaluation criteria for NIST post-quantum standardization process.
>
> 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 (or paragraph) 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 with practical attacks** 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 to validate those attacks. 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.
>
> Additionally, providing parameters with low and very low security levels is in the line of a long tradition in public-key cryptography where many systems have been proposed accompanied with parameters with low and very low security levels, asking the cryptographers to practically break the systems with those low-level security parameters.
>
> Best regards,
> Danilo!
> _____
> pqc-forum mailing list
> pqc-forum@nist.gov
> (_internal_name)s