From: D. J. Bernstein <djb@math.uic.edu>
Sent: Wednesday, May 7, 2025 11:39 AM
To: infoqual
Subject: Section 515 of Public Law 106-554
Attachments: signature.asc

Dear Director, NIST Management and Organization Office:

1. I am writing to you to submit a request under Section 515 of Public Law 106-554 for correction of information, as per the following
procedures:

https://web.archive.org/web/20250507112244/https://www.nist.gov/director/nist-information-quality-standards

My name is Daniel J. Bernstein. My address is Department of Computer Science, 851 S. Morgan St, MC 152, Chicago, IL, 60607. My email address is djb@math.uic.edu. Given the slowness and unreliability of postal services, please use email for all communication regarding this matter.

2. The particular information at issue is Table 5 in this document:

https://web.archive.org/web/20250313083030/https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf

This document, NIST IR 8545, was issued by NIST in March 2025 and is also currently available on the NIST web site. It was issued within NIST's Post-Quantum Cryptography Standardization Process, and lists pqc-comments@nist.gov as a contact address.

The aforementioned NIST project solicited four rounds of submissions, including software, with due dates in 2017, 2019, 2020, and 2022. There were various changes to the submissions, described in the submission documents and sometimes also as intermediate announcements on NIST's "pqc-forum" mailing list. For example,

https://web.archive.org/web/20250325060224/https://csrc.nist.gov/CSRC/media/Projects/post-quantum-cryptography/documents/round-2/official-comments/Classic-McEliece-round2-official-comment.pdf

shows that NIST received a public "OFFICIAL COMMENT" from Tung Chou in 2020 (during the second round) announcing a big software speedup for Classic McEliece, one of the submissions.

NIST IR 8545 says it evaluates the fourth-round submissions. In particular, Table 5 of NIST IR 8545 claims to be evaluating a cost metric ("cycles") for the Classic McEliece submission.

Now here's the problem in a nutshell: the number "114 189" in Table 5 of NIST IR 8545 is easily verified to be wrong, overstating cost in this metric by approximately a factor of 4.

More broadly, the numbers in that table are actually evaluations of the second-round Classic McEliece software. NIST is falsely portraying these numbers as evaluations of the fourth-round Classic McEliece software.

The source cited by NIST for the table already had a prominent warning in April 2024 that it was giving out-of-date numbers from a defunct measurement project:

https://web.archive.org/web/20240425050637/https://openquantumsafe.org/benchmarking/

NIST's bibliography entry violates the standard requirement of stating an access date. When I publicly challenged Table 5 (on a "pqc-forum"
mailing list operated by NIST), did NIST claim that, oops, it had visited the URL before the warning appeared, and hadn't rechecked for an entire year before issuing NIST IR 8545, and had somehow misled itself into believing that the data was for the round-4 software?

No. Instead NIST claimed "We have verified that the performance figures given in the tables in our report accurately reflect the benchmarks we
cited":

https://web.archive.org/web/20250507151442/https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/CSYRn8A-0zE/m/1PPIazqcAAAJ

This is absurd. The cited source doesn't claim to be, and isn't, measuring the round-4 submission. The claim that the numbers are measurements of the round-4 submission is a fabrication by NIST.

Along with claiming accuracy, NIST threw up a smokescreen, writing that "performance can vary significantly depending on factors such as platform, application, computing environment, and network conditions".
Those variations have nothing to do with the issue at hand.

NIST IR 8545 claims "114 189" kilocycles for mceliece348864f key generation on "x86_64". A closer look at "[1]" shows that this is from an Intel Xeon Platinum 8259CL CPU. The submitted fourth-round software is 4x faster than that on that CPU.

The network conditions and application are irrelevant. The problem is NIST claiming measurements of the fourth-round candidate when in fact NIST is talking about code from 2019, ignoring subsequent speedups.

3. Your procedures, beyond simply asking "why the requester believes that the information is not correct", also ask "how the information at issue fails to comply with applicable information quality guidelines and standards".

NIST IR 8545 does not comply with the following NIST information-quality standards. I am not saying that this list is complete, but this list is clearly sufficient for invoking Section 515 of Public Law 106-554.

3(a). "Quality will be ensured and established at levels appropriate to the nature and timeliness of the information to be disseminated."

As background, attackers are recording data encrypted today to decrypt with future quantum computers. Post-quantum cryptography is a multi-billion-dollar industry reacting to this security problem.

Various existing NIST standards have the same security problem. In 2016, NIST issued 81 FR 92787, establishing a multi-year process to evaluate and standardize replacements, and citing criteria that "will be used"
for that process. Those criteria include a statement that the goal of the process is to "select a number of acceptable candidate cryptosystems for standardization":

https://web.archive.org/web/20220119113311/https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

Evaluation of the acceptability of post-quantum cryptosystems is thus an important and urgent task.

NIST IR 8545 says that its purpose is to summarize "the fourth round of the NIST PQC Standardization Process". Unfortunately, in preparing the report, NIST recklessly collected round-2 information and falsely presented it as round-4 information, while ignoring and suppressing warnings about the information being out of date. This was neither ensuring nor establishing an appropriate level of quality.

Note that "quality" is defined to include "objectivity", which includes "a focus on ensuring accurate, reliable, and unbiased information", along with a procedural requirement of "sound statistical and research methods". What NIST did here was not sound research, and did not take reasonable steps to ensure accuracy.

3(b). "Although third-party sources may not be directly subject to Section 515, information from such sources, when used by NIST to develop information products or to form the basis of a decision or policy must be of known quality and consistent with the applicable information quality guidelines and standards. When such information is used, any limitations, assumptions, collection methods, or uncertainties concerning it are taken into account and disclosed."

NIST IR 8545 violated this "disclosed" rule by repeating numbers from a non-governmental source while suppressing the warning prominently provided by that source.

NIST IR 8545's failure to state an access date for the reference was another violation of this rule.

The "known quality" rule means that NIST cannot rely on ignorance as an excuse for repeating bad information. For example, if NIST suddenly decides to switch to claiming that it _assumed_ that these third-party numbers were measurements of the round-4 software: "known quality" means that NIST wasn't allowed to make any such assumption.

3(c). "Scientific and financial information disseminated by NIST is reliable and accurate to an acceptable degree of error as determined by factors such as the importance of the information, its intended use, time sensitivity, expected degree of permanence, relation to the primary
mission(s) of the disseminating office, and the context of the dissemination, balanced against the resources required and the time available."

See above regarding importance and time sensitivity. NIST IR 8545 is a permanent report, a prominent part of a multi-year multi-person project by the disseminating office at NIST, a project that has been repeatedly highlighted in activity reports by that office and that plays an indispensable role in White House orders regarding the topic.

NIST IR 8545 does not quantify the weights placed upon individual comparison factors, such as the specific table at issue; but it would not be credible for NIST to retroactively claim that Table 5 is an unimportant part of NIST IR 8545. The tables are prominently placed (this table is on page 6 of a 34-page document), appear to be the source of various comments in the text, and are the central cost measurements in the report. Cost is the second main evaluation criterion stated in NIST's evaluation criteria for the project:

https://web.archive.org/web/20220119113311/https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

NIST is obliged to follow those criteria by 81 FR 92787 unless and until that is overridden. More to the point, there is ample evidence of cost measurements playing a major role in cryptographic decisions.

Regarding "intended use", NIST appears to have now terminated activity under the name "Post-Quantum Standardization Process" (perhaps because of my ongoing FOIA lawsuits regarding that process). However, the stated goal to "select a number of acceptable candidate cryptosystems for standardization" has not disappeared. On the contrary, NIST and other standardization agencies are continuing to work on post-quantum standardization, as illustrated by

https://web.archive.org/web/20250415051610/https://csrc.nist.gov/Projects/pqc-dig-sig/

and by the following statement from NIST IR 8545: "After the ISO standardization process has been completed, NIST may consider developing a standard for Classic McEliece based on the ISO standard."

So it would not be credible for NIST to claim that the "intended use" of its evaluations of candidates is merely to document a past decision.
Furthermore, such a claim cannot retroactively justify NIST's recklessness in handling this data when it was making that decision.
NIST was violating the rules at that point, not taking reasonable steps to ensure accuracy.

Regarding the resources required to obtain the correct information, the correct numbers were stated in a table in

https://classic.mceliece.org/mceliece-impl-20221023.pdf#page.10

which was part of the fourth-round submission package filed with NIST.
Those numbers are for Intel Haswell CPUs; NIST had designated Haswell as its comparison platform in

https://web.archive.org/web/20220120140641/https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/BjLtcwXALbA/m/Bjj_77pzCAAJ

in 2019 and never announced a revised designation, although the NIST IR
8545 table at issue actually switches to newer Intel CPUs with slightly better numbers. Continually updated measurements for many CPUs are available from

https://bench.cr.yp.to

which is a long-running measurement project that I co-initiated and continue to manage. Verifying the accuracy of the numbers is a simple matter of re-running the software.

3(d). "NIST Policy 1800.00 requires that NIST measurement results be accompanied by quantitative statements of their uncertainty, and that a uniform approach to expressing measurement uncertainty be followed."

The tables in NIST IR 8545 fail to include this information. For comparison, the numbers from

https://classic.mceliece.org/mceliece-impl-20221023.pdf#page.10

include medians and quartiles, as do the https://bench.cr.yp.to tables.

3(e). "NIST treats information quality as integral to every step in its process of developing the information, including creation, collection, maintenance, and dissemination. All scientific information disseminated by NIST receives a level of scrutiny commensurate with the critical nature of the information and its intended use."

Obviously this scrutiny did not take place here. NIST copied and pasted third-party round-2 numbers and falsely presented those as round-4 numbers.

4. Your procedures also require "an explanation of how the requester is affected". By definition, "affected person" means "an individual or entity that uses, benefits from, or is harmed by the disseminated information at issue".

To answer this, I'll start by quoting the Policy Statement on Ethical Guidelines from the American Mathematical Society: "The correct attribution of mathematical results is essential, both because it encourages creativity, by benefiting the creator whose career may depend on the recognition of the work and because it informs the community of when, where, and sometimes how original ideas entered into the chain of mathematical thought." Specific responsibilities include giving "appropriate credit" and using "no language that suppresses or improperly detracts from the work of others":

https://www.ams.org/about-us/governance/policy-statements/sec-ethics

I am speaking for myself in this message, but I am also one of the members of the team that submitted Classic McEliece to NIST. What NIST is doing in the table at issue is exaggerating the cost, specifically the CPU time, of Classic McEliece. NIST is improperly detracting from the work of all of the scientists who contributed to Classic McEliece.

Furthermore, NIST's citation and usage of (obsolete) results from https://openquantumsafe.org/benchmarking/ fails to give appropriate credit to https://bench.cr.yp.to, a project that had the relevant benchmarks before anyone else, along with careful attention to accuracy, verifiability, comprehensiveness, etc.

Beyond my role as a scientist working in this area, I am like billions of other people in relying on cryptography to protect data in transit through the Internet. Classic McEliece has the strongest track record of all available options for post-quantum public-key encryption, and it is also the most efficient option for a large class of applications (what are called "static keys" in, e.g. NIST SP 800-56 and 800-57), contrary to what NIST IR 8545 indicates. I don't expect NIST's misinformation about Classic McEliece to be able to stop Classic McEliece deployment, but I do expect it to slow down deployment if it is not promptly corrected. Ultimately NIST is damaging security, damaging efficiency, and harming the general public.

5. Your procedures also say that you will not consider corrections that "would serve no useful purpose", such as corrections to information that is "not valid, used, or useful after a stated short period of time".

NIST IR 8545 does not state a time limit on the usage of its information regarding Classic McEliece. On the contrary, as noted above, there is ongoing activity by NIST and others regarding this. Consider again the following statement in NIST IR 8545: "After the ISO standardization process has been completed, NIST may consider developing a standard for Classic McEliece based on the ISO standard."

You can see from https://mceliece.org that there are already many users of Classic McEliece, and further users who have expressed interest in Classic McEliece. Cryptographic decisions are happening all the time.
There is no excuse for NIST misrepresenting what is known about the features of the options that are available.

6. I believe that a suitable form of correction would be an update to NIST IR 8545 to correct Table 5, accompanied by an apology for the indefensible previous misinformation from NIST.

Please let me know if you need any further information.

---D. J. Bernstein