UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-0001

August 4, 2025

Daniel J. Bernstein
Department of Computer Science
University of Illinois Chicago
851 S. Morgan St., MC 152
Chicago, IL 60607
Via email: djb@math.uic.edu

Dear Dr. Bernstein:

This letter is in response to your May 7, 2025 request for correction (Request) of certain information contained in the NIST IR 8545, Status Report on the Fourth Rounds of the NIST Post-Quantum Cryptography Standardization Process[1]. Your Request is submitted under the Information Quality Act, Section 515 of Public Law 106-554; the Office of Management Budget's Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (67 FR 8451, Feb. 22, 2002) ("OMB Guidelines"); the Office of Management and Budget's Memorandum on Improving Implementation of the Information Quality Act, M-19-15 ("OMB Memo"); and NIST's Guidelines, Information Quality Standards, and Administrative Mechanism ("NIST Guidelines").

The Request asserts that the following information in NIST IR 8545 requires correction:

1. That the number "114 189" in Table 5 is incorrect, overstating the number of clock cycles by approximately a factor of 4.
2. That this number incorrectly reflects performance of the second-round software for Classic McEliece, not the fourth-round implementation.
3. That NIST cited a defunct and unmaintained source without disclosing the limitations and omitted access dates for the citation.
4. That NIST disregarded better benchmarking sources, such as the SUPERCOP/bench.cr.yp.to platform, which is more accurate, current, and comprehensive.

You cite previous correspondence regarding the Table 5 number on a "pqc-forum" mailing list[2].

[1] Available at: https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf
[2] https://groups.google.com/u/1/a/list.nist.gov/g/pqc-forum/c/CSYRn8A-0zE/m/6rhWGzEgDgAJ

According to the Request, the supposed error misinformed the cryptographic community and delayed deployment of Classic McEliece, thereby impacting efficiency and public security.

NIST IRs are part of the NIST Technical Series Publication and defined as interagency or internal reports of research findings, including background information for Federal Information Processing Standards (FIPS) and NIST Special Publications (NIST SP)[3]. NIST treats NIST IRs as fundamental research communication. As stated in the NIST Guidelines, while fundamental research communications are expected to adhere to information aquality standards and do receive technical, policy, and editorial review by the NIST Editorial Review Board in addition to the pre-dissemination review methods listed in the NIST Guidelines, they are not included in the scope of the OMB and NIST Guidelines. NIST IR 8545 was approved by the NIST Editorial Review Board on March 5, 2025.

Even if, assuming *arguendo*, NIST IR 8545 were to be included within the scope of the NIST Guidelines, your requests for correction would not be warranted, as discussed below.

1. ***Request for Correction:*** *The number "114 189" in Table 5 is incorrect, overstating the number of clock cycles by approximately a factor of 4.*

   NIST recognizes that different benchmarking platforms have reported varying results using different implementations of the Classic McEliece algorithm, with some reporting lower cycle counts than those listed in Table 5. However, this figure in Table 5 was accurately cited from a publicly available benchmark source—specifically, Reference [1] in NIST IR 8545, which corresponds to the Open Quantum Safe (OQS) project[4]. NIST IR 8545 accurately reproduces the benchmark results published there. Importantly, only one out of 48 data points drawn from Reference [1] across Tables 3, 4, and 5 has been challenged, and even this challenged data point was correctly cited. The allegation that the report fabricated or misstated data is unfounded. As stated in NIST IR 8545, the performance figures are intended to be representative, not definitive, and reasonable differences in benchmark platforms or methodologies do not constitute misinformation.

2. ***Request for Correction:*** *This number reflects the performance of the second-round software for Classic McEliece, not the fourth-round software implementation.*

   NIST disagrees with this assertion. NIST is confident that the benchmarks cited from Reference [1] accurately reflect the fourth-round version of Classic McEliece. NIST IR 8545 focuses specifically on fourth-round submissions, and the benchmark data

[3]https://csrc.nist.gov/publications#:~:text=NIST%20Interagency%20or%20Internal%20Reports%20(NIST%20IR),NIST%20Cybersecurity%20and%20Privacy%20Program.
[4] Open Quantum Safe (OQS) algorithm performance visualizations. Available at https: //openquantumsafe.org/benchmarking

used aligns with that scope. Accordingly, the performance measurement in question is consistent with the version under evaluation.

3. ***Request for Correction:*** *NIST cited a defunct and unmaintained source without disclosing the limitations and omitted access dates for the cited source.*

   The cited source— Open Quantum Safe algorithm performance visualizations — was an active and widely used project at the time NIST gathered benchmark data. It played a visible and constructive role in the NIST post-quantum cryptography process. The disclaimer currently shown on the OQS website was added after NIST collected the data. NIST accurately cited the relevant information as it existed at the time. The addition of a later disclaimer does not retroactively invalidate the benchmark or its citation.

4. ***Request for Correction:*** *NIST disregarded better benchmarking sources, such as the SUPERCOP/bench.cr.yp.to platform, which is more accurate, current, and comprehensive.*

   Benchmarking results naturally vary depending on the platform, implementation, and methodology. As stated in the report, the benchmark tables were intended to provide representative data points, not authoritative or exhaustive metrics. NIST did not disregard SUPERCOP; it was among the sources NIST reviewed during the evaluation process. Ultimately, NIST selected Reference [1] because it provided a consistently structured and well-documented dataset that served NIST's goal of presenting a fair, representative comparison across submissions. NIST recognizes that experts may have different preferences for benchmarking sources, but choosing one over another for clarity and consistency does not imply negligence or bias.

Regarding the alleged harm, we emphasize that key generation cycle counts are only one of many considerations for weighing alternatives for standardization. Suitability and competitiveness of a given algorithm for standardization depend on a variety of security, performance, and implementation characteristics across different use cases. Improved key generation benchmarks alone would not change the conclusions.

Based on the foregoing, your Request is denied. In preparing this response, NIST carefully reviewed the relevant information and sources cited to ensure that its conclusions are accurate, well-founded, and consistent with NIST's information quality standards.

You may appeal this decision within 30 calendar days from the date of this decision. Such an appeal must be in writing and addressed to:

NIST Associate Director for Laboratory Programs
National Institute of Standards and Technology

100 Bureau Drive, Mail Stop 1000
Gaithersburg, MD 20899-1000

An appeal of an initial denial must include:

1. The requestor's name, current home or business address, and telephone number or e-mail address (to ensure timely communication);
2. A copy of the original request and any correspondence regarding the initial denial; and
3. A statement of the reasons why the requester believes the initial denial was in error.

Additional details regarding the appeal process can be found in Section D. of the NIST Guidelines.

Sincerely,

AMY EGAN

Digitally signed by AMY EGAN
Date: 2025.08.04 15:59:02 -04'00'

Amy Egan
Acting Director, Management and Organization Office