**From:** Ron Steinfeld <ron.steinfeld@monash.edu>
**Sent:** Thursday, December 27, 2018 9:40 PM
**To:** pqc-comments
**Cc:** pqc-forum@list.nist.gov
**Subject:** OFFICIAL COMMENT: Titanium

Dear pqc-forum,

We would like to inform you that an updated version of the Titanium specification document (version 1.1) is now available from the Titanium web page at

http://users.monash.edu.au/~rste/Titanium.html.

A summary of the updates in this version is included in Chapter 7 of the updated specification document. A brief summary is also included below.

Version 1.1 contains the following updates, some of which were reported at the First NIST PQC workshop in April 2018:

1. Constant time implementation improvements:
The implementation submitted to NIST may not be constant time depending on the C compiler implementation of % mod reduction operations. To address this, we rewrote the mod reduction code to avoid % operations and ensure a compiler-independent constant-time implementation. We also improved the efficiency of the NTT implementation. The updated implementation code is available at https://github.com/raykzhao/Titanium/

2. OpenQuantum integration:
Our updated implementation of Titanium was recently integrated into the Open Quantum Safe (liboqs) library. We have added our benchmark results for this integration and benchmark comparison with other liboqs schemes.

3. New AES-based PRG Titanium variant ("Titanium-AES"):
We added a new variant of Titanium (not in original NIST submission) which uses AES to replace the SHA-3 based PRG. This allows faster implementation on suitable CPU hardware using Intel AES-NI instructions.

4. Minor documentation corrections/clarifications: see Chapter 7 of the updated specification document for details.

Best Regards,

Ron Steinfeld, Amin Sakzad and Raymond K. Zhao (Titanium team)

--
Dr. Ron Steinfeld

Senior Lecturer,
Cybersecurity Lab,
Faculty of Information Technology,
Monash University,
Clayton VIC 3800
Australia

Email: ron.steinfeld@monash.edu
Phone: +61 3 99055225

Fax: +61 3 9905 5159
Web:
* Personal: http://users.monash.edu.au/~rste/
* Monash Cybersecurity Lab: http://www.monash.edu/cybersecurity-lab