From: vadim1980@gmail.com on behalf of Vadim Lyubashevsky <vadim.lyubash@gmail.com>
Sent: Friday, December 22, 2017 6:26 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: qTESLA

Dear Authors,

In Table 1, should |\Delta L| be ~ 2^{(d+1)n} instead of just 2^(d+1)? In Equation 7, the numerator is |\Delta L| and it's correctly stated as 2^{(d+1)n} there.

In the long equation in the middle of page 14, it looks as if you are correctly using |\Delta L|= 2^{(d+1)n}, but then it also looks as if you forgot to multiply by |\Delta S| because I don't see any B in there.

The main implication of having an incorrect |\Delta L| or forgetting to multiply by |\Delta S| is that it doesn't look that the condition needed for the qROM reduction from plain Ring-LWE can be satisfied (and so I don't think that Theorem 6 is correct ... I am not claiming that the scheme is insecure, though).

If I misunderstood something, I would be interested in seeing a more precise version; because having a Fiat-Shamir signature with a qROM reduction from plain Ring-LWE for such a small value of q would be a very interesting theoretical result.

Best,
-Vadim

From:	Patrick Longa Pierola <plonga@microsoft.com>
Sent:	Friday, June 15, 2018 10:58 AM
To:	pqc-comments
Cc:	pqc-forum@list.nist.gov
Subject:	[pqc-forum] OFFICIAL COMMENT: qTESLA

Dear All,

as we announced during the presentation of qTESLA at the NIST's First PQC Standardization Conference in April 2018, the qTESLA team has been working on the tuning of the parameter sets that were originally submitted to NIST on November 30, 2017, and on correcting the mistake pointed out by Vadim Lyubashevsky (pqc-forum message on 12/22/2017) that nullified the "provably-secure" property of our qTESLA instantiations.

As a result of this work, we are announcing today an update of our parameter sets as follows.

We are proposing the next parameter sets using two different approaches:

1) Three parameter sets "heuristic qTESLA", chosen using a heuristic approach and especially optimized for performance and key/signature size:

qTESLA-I: targeting NIST's security category 1.

qTESLA-III-speed: targeting NIST's security category 3, and optimized for speed.

qTESLA-III-size: targeting NIST's security category 3, and optimized for key/signature size.

2) Two parameter sets "provably-secure qTESLA", chosen according to a security reduction and intended for more conservative, high-security applications:

qTESLA-p-I: targeting NIST's security category 1.

qTESLA-p-III: targeting NIST's security category 3.

The "heuristic qTESLA" parameter sets above replace the originally submitted parameter sets qTESLA-128, qTESLA-192 and qTESLA-256. These new parameter sets are essentially finely-tuned versions that match more closely NIST's definition of security categories. As a result they achieve a significantly improved performance.

The new "provably-secure qTESLA" parameter sets are generated by correcting the typo in the original parameter generation script. Their security is supported by qTESLA's security reduction in the (quantum) random oracle model.

In the process, we have also made significant improvements to our C-only reference implementations, have corrected some parts in the code that were not properly protected against timing and cache attacks, and have improved some design features of the scheme, for example, to add resilience against certain fault attacks. (We especially thank Peter Pessl and Matthias Kannwischer for their comments and suggestions that helped us improve a previous version of the software).

Below we show some results that summarize the performance obtained with the recent updates.

Performance in kilocyles on an Intel Core-i7 6700 (Skylake) processor

	keygen	sign	verify	total (sign + verify)
qTESLA-I :	1 583	467	99	566

qTESLA-III-speed :	3 576	663	202	864
qTESLA-p-I :	6 678	1 259	505	1 763

We note that the parameter sets proposed in this update only target NIST's categories 1 and 3. We might propose additional parameter sets targeting other security levels in the near future. We are also working on optimized implementations exploiting assembly, and will report the results soon.

Finally, we also announce a brand new website for qTESLA: qtesla.org

In this website, we have posted links to the updated and much improved specifications document:

https://qtesla.org/wp-content/uploads/2018/06/qTESLA_v2.0_06.14.2018.pdf

To the full updated submission package:

https://qtesla.org/wp-content/uploads/2018/06/qTESLA_NIST_update_06.14.2018.zip

And to the reference software:

https://github.com/qtesla/qTesla

We respectfully leave to NIST the decision of accepting these changes in this first round of the PQC standardization process. Otherwise, in case qTESLA qualifies, we would like to ask NIST to consider the improvements for a second round.

Sincerely,
The qTESLA team

From: Patrick Longa Pierola <plonga@microsoft.com>
Sent: Monday, July 02, 2018 2:56 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: qTESLA

Dear All,

We have made a few small changes to the spec document and reference implementation. The updated package is available here:

https://qtesla.org/wp-content/uploads/2018/07/qTESLA_NIST_update_06.30.2018.zip

And the updated document is available here:

https://qtesla.org/wp-content/uploads/2018/07/qTESLA_v2.1_06.30.2018.pdf

Here is a summary of the changes:

- Fixed a few typos in the document.
- (Small) tightening of the bounds of the signature rejection evaluation, line 18 of Algorithm7.
- Updated correctness proof in Section 2.3.
- The order of the signature and signed message was changed in the “signature package” (signature now goes in the lowest address position). Updated KATs accordingly.

Sincerely,
The qTESLA team

From: Patrick Longa <plonga@microsoft.com>
Sent: Wednesday, August 29, 2018 2:18 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] OFFICIAL COMMENT: qTESLA

Dear All,

We have made a few minor improvements to the code and spec document, including some minor corrections. The updated package is available here:

https://qtesla.org/wp-content/uploads/2018/08/qTESLA_NIST_update_08.27.2018.zip

And the updated spec document is available here:

https://qtesla.org/wp-content/uploads/2018/08/qTESLA_v2.2_08.27.2018.pdf

We have also updated the reference implementation in qTESLA's GitHub repository:

https://github.com/qtesla/qTesla

Here is a summary of the changes:

- Corrected typo in the definition of mod±.
- Corrected typo in the signature verification algorithm, line 6 of Algorithm 8.
- Corrected typos in Algorithm 10 (function "GenA"). Rearranged if-blocks to maximize use of cSHAKE128's output. Updated KATs accordingly.
- Corrected typos in Algorithm 13 (function "Enc"). Rearranged if-blocks to maximize use of cSHAKE128's output.
- Added rejection of value B + 1 during sampling of y, Algorithm 14.

Sincerely,
The qTESLA team