**From:** Kerman, Sara J. (Fed)
**To:** Calik, Cagdas (IntlAssoc); McKay, Kerry A. (Fed); Sonmez Turan, Meltem (Fed)
**Cc:** lightweight-crypto
**Subject:** web page updates
**Date:** Wednesday, April 24, 2019 3:24:32 PM

I've updated the website with the following and requested publishing (not sure if Jim has left for the day):

ROUND 1
Added KNOT official comment
Added zip file to "download all files"

MAIN PROJECT PAGE – added a link the test vector zip file
"NIST has published a call for algorithms (test vector generation code) to be considered for lightweight cryptographic standards"

Sara

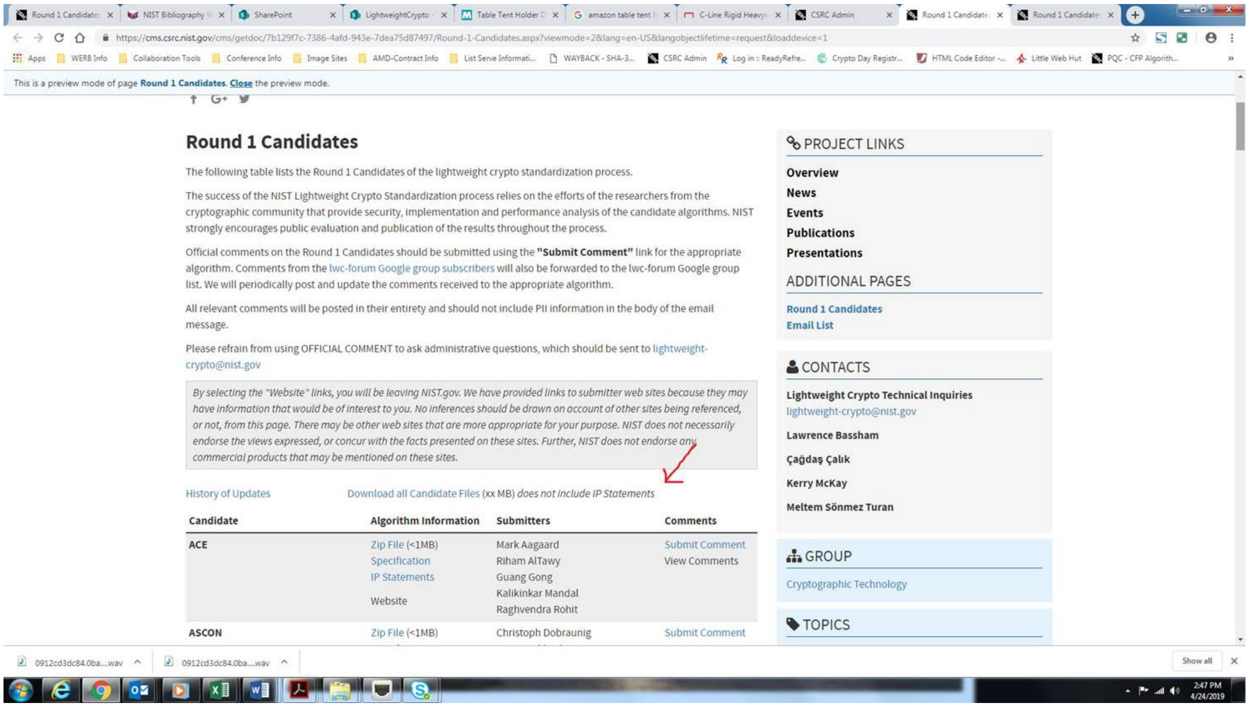
**From:** Calik, Cagdas (IntlAssoc)
**Sent:** Wednesday, April 24, 2019 2:56 PM
**To:** Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
**Subject:** RE: forum requests

The place is fine. Would "Download all Zip Files" be a better name?

Cagdas

**From:** Kerman, Sara J. (Fed)
**Sent:** Wednesday, April 24, 2019 2:52 PM
**To:** McKay, Kerry A. (Fed) <kerry.mckay@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>
**Subject:** RE: forum requests

Should I put the "Download All Candidate Files" link here?  Note, they do not include IP statements because they were kept separate from the submission folders.



https://cms.csrc.nist.gov/cms/getdoc/7b129f7c-7386-4afd-943e-7dea75d87497/Round-1-Candidates.aspx?viewmode=2&lang=en-US&langobjectlifetime=request&loaddevice=1

This is a preview mode of page **Round 1 Candidates**. **Close** the preview mode.

## Round 1 Candidates

The following table lists the Round 1 Candidates of the lightweight crypto standardization process.

The success of the NIST Lightweight Crypto Standardization process relies on the efforts of the researchers from the cryptographic community that provide security, implementation and performance analysis of the candidate algorithms. NIST strongly encourages public evaluation and publication of the results throughout the process.

Official comments on the Round 1 Candidates should be submitted using the **"Submit Comment"** link for the appropriate algorithm. Comments from the lwc-forum Google group subscribers will also be forwarded to the lwc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Please refrain from using OFFICIAL COMMENT to ask administrative questions, which should be sent to lightweight-crypto@nist.gov

*By selecting the "Website" links, you will be leaving NIST.gov. We have provided links to submitter web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites.*

History of Updates    Download all Candidate Files (xx MB) *does not include IP Statements*

| Candidate | Algorithm Information | Submitters | Comments |
|---|---|---|---|
| **ACE** | Zip File (<1MB)<br>Specification<br>IP Statements<br>Website | Mark Aagaard<br>Riham AlTawy<br>Guang Gong<br>Kalikinkar Mandal<br>Raghvendra Rohit | Submit Comment<br>View Comments |
| **ASCON** | Zip File (<1MB) | Christoph Dobraunig | Submit Comment |

PROJECT LINKS
**Overview**
**News**
**Events**
**Publications**
**Presentations**

ADDITIONAL PAGES
**Round 1 Candidates**
**Email List**

CONTACTS
**Lightweight Crypto Technical Inquiries**
lightweight-crypto@nist.gov
**Lawrence Bassham**
**Çağdaş Çalık**
**Kerry McKay**
**Meltem Sönmez Turan**

GROUP
Cryptographic Technology

TOPICS

**From:** McKay, Kerry A. (Fed)
**Sent:** Wednesday, April 24, 2019 2:23 PM
**To:** Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; lightweight-crypto <lightweight-crypto@nist.gov>
**Subject:** Re: forum requests

That sounds reasonable to me. Draft for HYENA team below.

-Kerry

Dear HYENA team,

Thank you for letting us know about the error. We are not allowing updates to the Round 1 candidate submission packages at this time. We encourage teams to host their own websites where they can make updates and corrections to their submission packages available. For example, some teams have decided to make them available on GitHub.

We also recommend that you let the forum know that there was an error in your specification.

**From:** "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
**Date:** Wednesday, April 24, 2019 at 1:58 PM
**To:** "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>, "Calik, Cagdas (IntlAssoc)" <cagdas.calik@nist.gov>, lightweight-crypto <lightweight-crypto@nist.gov>
**Subject:** RE: forum requests

Yes, that is my understanding. We do not accept changes to the code/specification at this moment. So, zip file will not be updated either.

Kerry does this sound reasonable? Kerry, can you draft a reply to hyena team? We are preparing the escapee room now. : ))

**From:** Kerman, Sara J. (Fed)
**Sent:** Wednesday, April 24, 2019 1:53 PM
**To:** Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>; Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; lightweight-crypto <lightweight-crypto@nist.gov>

**Subject:** RE: forum requests

It's not difficult, but in speaking to Kerry yesterday, it sounded like we weren't going to offer that because anyone that makes changes means updating all the files related to that algorithm and then the full zip file.   Has that changed now?

Also, what is happening with HYENA that sent in corrections to their files?  I seem to recall with PQC we asked people to post updated versions/changes to their website.

Sara

---

**From:** Sonmez Turan, Meltem (Assoc)
**Sent:** Wednesday, April 24, 2019 1:49 PM
**To:** Calik, Cagdas (IntlAssoc) <cagdas.calik@nist.gov>; lightweight-crypto <lightweight-crypto@nist.gov>
**Subject:** RE: forum requests

Sara,

Is it easy to construct a zip file that contains all files?

Thanks,
Meltem

---

**From:** Calik, Cagdas (IntlAssoc)
**Sent:** Wednesday, April 24, 2019 1:25 PM
**To:** lightweight-crypto <lightweight-crypto@nist.gov>
**Subject:** forum requests

We have a couple of questions/requests received via the lwc-forum:

- Maria Eichlseder's question about the proper citation of the submission papers
- Luan Cardoso dos Santos's request to provide a zip file that contains all the submissions
- Michael Tempelmeier's question about the source files
    - Proposed a draft reply

Cagdas