From: Cfrg on behalf of Scott Fluhrer (sfluhrer)
To: Blumenthal, Uri - 0553 - MITLL; cfrg@irtf.org
Subject: Re: [Cfrg] NIST Report on 1st Round of PQ Algorithms
Date: Thursday, January 31, 2019 7:26:41 PM

I believe that's because NIST didn't ask for an AKE; only KEMs, public key encryption and signature algorithms.

I believe that NISTs reasoning was "let's nail down the most basic and most commonly used primitives first; then we can worry about the fancier ones (such as AKE, IBE, (partially) homeomorphic encryption, etc)"

Now, I suppose someone could have submitted a KEM with a side input that would act as an AKE; however, no one did...

> -----Original Message-----
> From: Cfrg <cfrg-bounces@irtf.org> On Behalf Of Blumenthal, Uri - 0553 -
> MITLL
> Sent: Thursday, January 31, 2019 4:24 PM
> To: cfrg@irtf.org
> Subject: Re: [Cfrg] NIST Report on 1st Round of PQ Algorithms
>
> I personally am surprised that there are no AKE schemes - only KEM (and
> while you can construct an AKE from a KEM, it's usually non-trivial and
> expensive).
>
> Any idea why AKE weren't submitted...?
>
> On 1/31/19, 13:47, "Cfrg on behalf of Joachim Strömbergson" <cfrg-
> bounces@irtf.org on behalf of joachim@strombergson.com> wrote:
>
>   Aloha!
>
>   On 2019-01-31 16:51, Russ Housley wrote:
>   > NIST just posted NISTIR 8240, the Status Report on the First Round of
>   > the NIST Post-Quantum Cryptography Standardization Process. It is
>   > available at https://doi.org/10.6028/NIST.IR.8240.
>
>   And here is the list of candidates moving to the second round:
>
>   https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-
> candidates
>
>   >From the page:
>
>   The 17 Second-Round Candidate public-key encryption and
>   key-establishment algorithms are:
>   BIKE
>   Classic McEliece
>   CRYSTALS-KYBER
>   FrodoKEM
>   HQC
>   LAC
>   LEDAcrypt (merger of LEDAkem/LEDApkc)
>   NewHope
>   NTRU (merger of NTRUEncrypt/NTRU-HRSS-KEM)
>   NTRU Prime
>   NTS-KEM
>   ROLLO (merger of LAKE/LOCKER/Ouroboros-R)
>   Round5 (merger of Hila5/Round2)
>   RQC
>   SABER
>   SIKE
>   Three Bears
>
>
>   The 9 Second Round Candidates for digital signatures are:
>   CRYSTALS-DILITHIUM
>   FALCON
>   GeMSS
>   LUOV
>   MQDSS
>   Picnic
>   qTESLA
>   Rainbow
>   SPHINCS+
>
>
>   --
>   Med vänlig hälsning, Yours
>
>   Joachim Strömbergson - Alltid i harmonisk svängning.
>
> ==
> ==============
>
>   ____
>   Cfrg mailing list
>   Cfrg@irtf.org
>   https://na01.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fwww.irtf.org%2Fmailman%2Flistinfo%2Fcfrg&amp;data=02%7C01%7Cquynh.dang%40nist.gov%7Ce8201ce0b1d54991b84108d687dbee46%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C636845776001237261&amp;sdata=8FsVEsIQ%2Bas%2B%2Fy1cQp6KBu4Lo0tybyV6hRpTWdn3KtA%3D&amp;reserved=0
>

____
Cfrg mailing list
Cfrg@irtf.org
https://na01.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fwww.irtf.org%2Fmailman%2Flistinfo%2Fcfrg&amp;data=02%7C01%7Cquynh.dang%40nist.gov%7Ce8201ce0b1d54991b84108d687dbee46%7C2ab5d82fd8fa4797a93e054655c61dec%7C1%7C0%7C636845776001237261&amp;sdata=8FsVEsIQ%2Bas%2B%2Fy1cQp6KBu4Lo0tybyV6hRpTWdn3KtA%3D&amp;reserved=0