From: Moody, Dustin (Fed)
To: Cooper, David (Fed)
Subject: Re: Selection of Third-Round Candidates
Date: Thursday, June 18, 2020 1:38:16 PM

That sounds right.

From: David A. Cooper <david.cooper@nist.gov>
Sent: Thursday, June 18, 2020 12:26 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Selection of Third-Round Candidates

Hi Dustin,

Thanks for the input. I guess Round 5's plain LWE vs. FrodoKEM was another example of something eliminated for performance reasons.

I don't think eliminated as a result of security concerns only applies to those that were "broken." Section 2.2.1 says:

> During the first and second rounds of the NIST standardization process, a number of cryptanalytic results dramatically reduced the security of some submitted schemes, and undermined NIST's confidence in the maturity of others. These results were the basis for many of NIST's decisions thus far in the process.

It seems that LAC and Round 5 had minor security issues that undermined our confidence in the schemes. Three Bears doesn't quite fit, but we had a security concern resulting from the lack of analysis.

In any case, it does seem we eliminated a lot of candidates because we had concerns, for one reason or another, about security. Of the remaining candidates only a few were eliminated because they were similar to another candidate, but had worse performance. I don't think we should say how many were eliminated for security concerns and how many were beat out in performance. However, it seems that we advanced almost every scheme that didn't have a security concern, and then used performance and other (e.g., IP) issues to decide which were finalists and which were alternates.

Thanks,

David

On 6/18/20 12:04 PM, Moody, Dustin (Fed) wrote:

> David,
> You have Three Bears, LAC, and Round5 in red.
>
> I'd say LAC and Round5 had some minor security issues, but were not "broken".
> They both had good performance, but we eliminated them mainly because we

don't have as much confidence in their overall submission - especially compared to the finalists. I also think Round5's plain LWE version wasn't as favorable as FrodoKEM in performance, but that's going from my memory.

Three Bears didn't have real security issues. It also had good performance, but our main reason is that we don't feel it has been analyzed enough by third parties.

I'd say performance was more of a factor in terms of schemes being alternate candidates, rather than finalists. SIKE is a good case of this. If SIKE was efficient, it very well might be a finalist. FrodoKEM is an alternate, in part because it is slower/bigger than the finalists. Same for BIKE, HQC, GeMSS, SPHINCS+, and PICNIC to some degree. There might be other issues, but performance being slow/bigger was certainly a factor in them being alternates as opposed to finalists.

These are my quick thoughts...

Dustin

From: David A. Cooper <david.cooper@nist.gov>
Sent: Thursday, June 18, 2020 11:55 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Selection of Third-Round Candidates

All,
As Dustin requested, I am working on revising Section 2.3 on the selection of the third-round finalists and alternative candidates. The current text talks about how performance was more of a consideration in the second round. However, I am trying to understand to what degree that was the case.
Below is a table of all of the second-round candidates (except NTS-KEM). I marked in blue the ones that are advancing to the third round, and I marked in red those that I thought were eliminated as a result of security concerns (please correct me where I am wrong). Unless I made a mistake about which ones were eliminated for security reasons, that leaves NewHope as the only candidate that was eliminated for performance reasons. (No, I do not think we add NewHope back in.) So, other than NewHope, was performance used for any reason other than deciding whether a third-round candidate would be a finalist or an alternate?
Thanks,
David

KEMs	Signatures
Kyber	Dilithium
Saber	qTesla
FrodoKEM	Falcon

Round 5	
LAC	SPHINCS+
NewHope	Picnic
Three Bears	
NTRU	LUOV
NRTUprime	Rainbow
	GeMSS
SIKE	MQDSS
Classic McEliece	
BIKE	
HQC	
LEDAcrypt	
ROLLO	
RQC	