From: Moody, Dustin (Fed)
To: Apon, Daniel C. (Fed); internal-pqc
Subject: RE: Comment on Saber (Mod-LWE vs Mod-LWR)
Date: Tuesday, April 9, 2019 1:34:00 PM

Quick update:

I checked with SABER, and it was a typo. They meant Mod-LWR.

From: Apon, Daniel C. (Fed)
Sent: Tuesday, April 9, 2019 1:33 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Comment on Saber (Mod-LWE vs Mod-LWR)

Sorry for the spam; important typo:

"as the case of bounded-samples, i.e. PRFs…"

should read

"as the case of **un**bounded-samples, i.e. PRFs…"

From: Apon, Daniel C. (Fed)
Sent: Tuesday, April 9, 2019 1:32 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Comment on Saber (Mod-LWE vs Mod-LWR)

Hi all,

Apparently I forgot to check Saber for completeness (I only saw 4 things to review, but I guess I had 5). Anyway, Saber's submission for the 2nd Round is complete from what I see.

Also, while I'm thinking about Saber, there was a comment that more cryptanalysis of Mod-LWR would be useful (and whether they actually meant security from Mod-LWE or Mod-LWR).
I checked back on this, and the 2nd Round Saber submission has a theorem (6.1) that shows security from Mod-LWR, without discussion or proof.
If you go back to their conference paper at AFRICACRYPT 2018, https://eprint.iacr.org/2018/230.pdf, they give a more in-depth proof, along with a justification (by citation) for their use of Mod-LWR as an assumption on its own.
The state of the art on Mod-LWE vs Mod-LWR (which the Saber team cites) is ultimately https://eprint.iacr.org/2016/589.pdf by Jacob and I.

So, for some parameter choices, it's true that the Saber scheme would have security from Mod-LWE. But of course – as everyone seems to have done with lattices – the actual parameters are instantiated based on their

best estimates of known attacks than based on provable security theorems (which are generally believed to be somewhat loose, so this hasn't been objectionable in general).

Anyway, the key point is that – in the regime of bounded-samples – Mod-LWE and Mod-LWR should be viewed as the same problem (as the case of bounded-samples, i.e. PRFs, is the only theoretical justification for treating them separately in the first place).
So my take is that the Saber team has as much justification to claim security from Mod-LWE as any lattice scheme has justification to claim security from X-LWE.
That is -- Sure, the parameters are chosen too tightly for the best-known reductions to apply, but you could just increase the parameters (mainly the modulus size(s)) and some reduction goes through – plus we think the reductions are themselves loose.
And on the other hand, they could just say "Mod-LWR" instead of "Mod-LWE;" there's no real difference that we know of.

And last, yes – it would still be nice to have some further fine-grained cryptanalysis of the concrete parameter choices of lattice schemes, but this mostly seems hard to do still

--Daniel