From: Moody, Dustin (Fed)
To: Robinson, Angela Y. (Fed); Kelsey, John M. (Fed); internal-pqc
Subject: Re: Rethinking ROLLO
Date: Thursday, June 4, 2020 9:47:21 PM

My preference would not be to add back in schemes. We need to make cuts - we can't keep everything. We can emphasize the positives about ROLLO and strongly encourage work in this direction. But they will need more time to achieve stability.

Maybe a good way to handle this would be to describe the on-ramp more generally, which could allow for either signatures or KEMs. We then emphasize that in particular we would be interested in a signature scheme which isn't structured lattice.

Any other thoughts?

Dustin

From: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Sent: Thursday, June 4, 2020 6:36 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Rethinking ROLLO

I suppose Three Bears would fall in that category. Are any other schemes in this category?

Sent from Mail for Windows 10

From: Kelsey, John M. (Fed)
Sent: Thursday, June 4, 2020 5:31 PM
To: Robinson, Angela Y. (Fed); internal-pqc
Subject: Re: Rethinking ROLLO

Angela,

I suspect the submitters of the still-unbroken lattice KEMs with better performance profiles than ROLLO would be pretty upset if we cut them and don't cut something that actually got broken.

--John

From: "Robinson, Angela Y. (Fed)" <angela.robinson@nist.gov>
Date: Thursday, June 4, 2020 at 16:05
To: internal-pqc <internal-pqc@nist.gov>
Subject: Rethinking ROLLO

Since I was tasked to write the ROLLO blurb in our report, I started taking a closer look at ROLLO. I'm

now wondering if we can save ROLLO.

ROLLO I is a CPA-secure KEM and ROLLO II is a CCA2-secure PKE. ROLLO I has smaller keys than the old BIKE numbers (old BIKE was aiming for CPA security) and ROLLO II's new numbers are comparable to the new BIKE numbers (new BIKE is aiming for CCA security).

		Public Key (B)	Ciphertext (B)
Level 1	BIKE	1,541	1,573
	ROLLO II	1,941	2,089
Level 3	BIKE	3,083	3,115
	ROLLO II	2,341	2,469

The obvious issue is the major and recent attacks on ROLLO. The development of the algebraic attacks broke all of old ROLLO's parameter sets except for ROLLO I, category 5. The question is, are more devastating attacks coming?

Although we have discussed an "on-ramp" for signatures, we don't plan to have one for KEMS. I think it's worth hanging on to ROLLO through the third round.

Thoughts?
Angela