From: Alperin-Sheriff, Jacob (Fed)
To: Jordan, Stephen P (Fed); Moody, Dustin (Fed); internal-pqc
Subject: Re: Regarding GuessAgain
Date: Wednesday, December 20, 2017 11:00:50 AM

Nice!

From: "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>
Date: Wednesday, December 20, 2017 at 9:52 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Regarding GuessAgain

Sure, ok.

Stephen

From: Moody, Dustin (Fed)
Sent: Wednesday, December 20, 2017 8:43 AM
To: internal-pqc
Subject: FW: Regarding GuessAgain

From: Alagic, Gorjan (Assoc)
Sent: Wednesday, December 20, 2017 8:43 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>
Subject: RE: Regarding GuessAgain

I looked at the spec again. I think it's true that they specify a public-key encryption algorithm, and that they claim IND-CCA2 security. If their implementation is also functioning properly, then I have no objection to letting them in.

Gorjan

From: Moody, Dustin (Fed)
Sent: Wednesday, December 20, 2017 8:18 AM
To: Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Alagic, Gorjan (Assoc) <gorjan.alagic@nist.gov>
Subject: FW: Regarding GuessAgain

What do you guys think?

From: Alperin-Sheriff, Jacob (Fed)
Sent: Tuesday, December 19, 2017 5:14 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Regarding GuessAgain

So the Asymmetric QC-MDPC code was unsalvageably incomplete/improper. However, desperate to salvage my goal number of submissions, I made Ray check over GuessAgain with me.

Other than the nonsensical unconditional security claim (which does not affect completeness or properness, and as they specifically discuss IND-CCA2 security and offer some sort of proof which may be nonsense, but irrelevant to completeness and properness), there is in fact nothing wrong with it

Stephen was incorrect that they didn't give our algorithm. Although they do describe part of their protocol as something else and some weird stuff, they do, in fact mention that they offer a public-key encryption scheme and, checking the implementation code, they have in fact built what appears to be a properly coded (unlike the Kayawood cheating) public key encryption scheme built out of the Alice end of the protocol. It may be insecure (I assume it is), the KATs match, they discuss security strengths/etc/etc.

If we're gonna throw them out for the unconditional nonsense we gotta throw out a number of other ones where they disagreed with our complaints re: security, and if we're gonna throw them out for describing as a key exchange protocol, we gotta throw Jintai (among others) out too, which we are really not gonna do.

Ray agrees with this (minus my zeal for the perfect number of submissions), so I'm gonna go ahead and upload it.

If you really want to ruin my dreams, I guess we can talk about it tomorrow.

—Jacob Alperin-Sheriff