**From:** Perlner, Ray (Fed)
**To:** Moody, Dustin (Fed); Alperin-Sheriff, Jacob (Fed)
**Subject:** RE: RVB response
**Date:** Wednesday, August 16, 2017 2:36:00 PM

Also, keep in mind that we left ourselves some flexibility for backburnering things we think aren't well studied enough. From the CFP:

"Algorithms that are not included in the narrowed pool
may still be considered for standardization at a later date, unless they are explicitly
removed from consideration by NIST."

That said, if the attack still works, we will almost certainly see another paper pointing this out before we have to make a decision.

**From:** Moody, Dustin (Fed)
**Sent:** Wednesday, August 16, 2017 2:25 PM
**To:** Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
**Subject:** RE: RVB response

I don't think we need to spend much time on this. I don't know that we'll need to explain why certain algorithms didn't move on. I think we'll mainly need to explain why certain ones did move on.

**From:** Alperin-Sheriff, Jacob (Fed)
**Sent:** Wednesday, August 16, 2017 2:23 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
**Subject:** Re: RVB response

I mean we're still not going to move this thing past the first round, right? Like this area of problems even on the chance they're right and that paper is wrong is still lacking in enough research for us to have any confidence in it.

I guess question is what do we write when justifying not moving algorithms past the first round …

**From:** "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
**Date:** Wednesday, August 16, 2017 at 2:19 PM
**To:** "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
**Subject:** RVB response

Ray, Jacob,

I don’t know if you ever saw this.  Here is their response as to the other papers they seem to indicate the RVB scheme is broken.  Also attached is an updated version of their scheme, for what it’s worth.

Dustin