From: Alperin-Sheriff, Jacob (Fed)
To: Moody, Dustin (Fed)
Subject: Re: 2nd round tweaks
Date: Thursday, December 13, 2018 11:03:57 AM

Let me post the microcontroller/programmable hardware thing first and get back to you tomorrow taking any responses into account.

.

From: "Moody, Dustin (Fed)"
Date: Thursday, December 13, 2018 at 11:01 AM
To: "Alperin-Sheriff, Jacob (Fed)"
Subject: RE: 2nd round tweaks

Can you write a paragraph stating our guidance/requirements? As a baseline, we say we're keeping with the requirements in the CFP so you'd only need to point out what we want different, and what we are encouraging.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, December 13, 2018 10:59 AM
To: Moody, Dustin (Fed) ; Bassham, Lawrence E. (Fed)
Cc: Perlner, Ray (Fed)
Subject: Re: 2nd round tweaks

Oh, we obviously do still want an ANSI C reference implementation for any tweaks, but no need for it to be optimized.
(AVX2/Haswell is implemented by AMD as well as Intel for x86 so it's not endorsing a company or product)

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Thursday, December 13, 2018 at 10:56 AM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Bassham, Lawrence E. (Fed)" <lawrence.bassham@nist.gov>
Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: 2nd round tweaks

My view.

> At this point, I think I would like to dispense with ANSI C for optimized implementation, I was never 100% on board with it.
> Instead we should note that we've been encouraging hardware-optimized implementations throughout the year and now STRONGLY RECOMMEND teams send us an official AVX2 (Haswell) optimized implementation (which can be the AVX2 in their original submission if they included one and don't plan to do any tweaks), regardless of whether or not they plan to do any tweaks.
> We should also say that we welcome any other hardware-optimized implementations, especially on programmable hardware and microcontrollers, but leave out the "STRONGLY RECOMMEND" language there.

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, December 13, 2018 at 10:45 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E.

(Fed)" <lawrence.bassham@nist.gov>

Cc: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>

Subject: 2nd round tweaks

Jacob and Larry,

I'm writing up a post with more detailed instructions for submitting tweaks to us (for the 2nd round candidates). Is there anything we need to say or anything regarding implementations? They'll be required to follow our original CFP, and so need to give us a reference implementation and optimized implementation for their updated scheme. Do we still want both? Do we want to change anything (like no vector instructions)? Any guidance as performance will be more important this round?

Dustin