

From: [Bassham, Lawrence E \(Fed\)](#)
To: [Alperin-Sheriff, Jacob \(Fed\)](#)
Subject: Re: A Submission Includes an Intrinsic using-version of AES-CTR (Saber).
Date: Wednesday, December 13, 2017 6:07:55 PM

It should be fairly equivalent, but it would be great if you could direct them to use the OpenSSL version.

On: 13 December 2017 15:46, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov> wrote:

I told them it was okay already but maybe I shouldn't have. ... Larry can you tell me what you think?

—Jacob Alperin-Sheriff