

From: [Moody, Dustin \(Fed\)](#)
To: (b) (6)
Subject: RE: Kerus
Date: Thursday, December 14, 2017 1:45:00 PM

Ray has some attacks on a couple. If you have an attack, write something down that we can send to the submitter and give them the option to comment/withdraw or whatever.

From: Daniel Smith (b) (6)
Sent: Thursday, December 14, 2017 1:07 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Kerus

Wow Kerus is bad. I can break it by hand. Give me more of these. FYI, I can also break the 256-bit parameters of DAGS and DME, so these are not well done either. Should we be breaking these yet?