From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed)
Subject: Dan"s quantum pre-image paper
Date: Monday, August 21, 2017 4:26:54 PM

The abstract of

https://eprint.iacr.org/2017/789.pdf

says:

NIST has claimed a high post-quantum security level for AES-128, starting from the following rationale: “Grover’s algorithm requires a longrunning serial computation, which is difficult to implement in practice. In a realistic attack, one has to run many smaller instances of the algorithm in parallel, which makes the quantum speedup less dramatic.” NIST has also stated that resistance to multi-key attacks is desirable; but, in a realistic parallel setting, a straightforward multi-key application of Grover’s algorithm costs more than targeting one key at a time. This paper introduces a different quantum algorithm for multi-target preimage search. This algorithm shows, in the same realistic parallel setting, that quantum preimage search benefits asymptotically from having multiple targets. The new algorithm requires a