From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed)
Subject: code-based paper
Date: Wednesday, May 25, 2022 2:14:10 PM

Ray,

I think this is the paper the invited talk for Code-based crypto workshop is based on.

https://eprint.iacr.org/2021/1634.pdf

> McElieceneedsaBreak–SolvingMcEliece-1284 andQuasi-Cyclic-2918withModernISD
>
> McElieceneedsaBreak–SolvingMcEliece-1284 andQuasi-Cyclic-2918withModernISD AndreEsser1,AlexanderMay 2*,andFloydZweydinger 1 CryptographyResearchCenter,TechnologyInnovationInstitute,UAE andre.esser@tii.ae 2 RuhrUniversityBochum,Germany {alex.may,floyd.zweydinger}@rub.de Abstract.
>
> eprint.iacr.org