From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed)
Subject: references
Date: Thursday, June 18, 2020 8:35:05 AM

Ray,

I asked Thinh to work on references. He suggested a whole bunch for BIKE (see below). I don't think we probably need this many. Can you let me know which (if any) we should cite in the BIKE write up?

Thanks,

Dustin

[42] Peters, Christiane. "Information-set decoding for linear codes over Fq." *International Workshop on Post-Quantum Cryptography*. Springer, Berlin, Heidelberg, 2010.

[43] Overbeck, Raphael, and Nicolas Sendrier. "Code-based cryptography." *Post-quantum cryptography*. Springer, Berlin, Heidelberg, 2009. 95-145.

[44] Canteaut, Anne, and Florent Chabaud. "A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511." *IEEE Transactions on Information Theory* 44.1 (1998): 367-378.

[45] Stern, Jacques. "A method for finding codewords of small weight." *International Colloquium on Coding Theory and Applications*. Springer, Berlin, Heidelberg, 1988.

[46] van Tilburg, Johan. "On the McEliece public-key cryptosystem." *Conference on the Theory and Application of Cryptography*. Springer, New York, NY, 1988.

[47] Lee, Pil Joong, and Ernest F. Brickell. "An observation on the security of McEliece's public-key cryptosystem." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1988.

[48] Leon, Jeffrey S. "A probabilistic algorithm for computing minimum weights of large error-correcting codes." *IEEE Transactions on Information Theory* 34.5 (1988): 1354-1359.

[49] Prange, Eugene. "The use of information sets in decoding cyclic codes." *IRE Transactions on Information Theory* 8.5 (1962): 5-9.

BIKE decoders

[50] Sendrier, Nicolas, and Valentin Vasseur. "About low DFR for QC-MDPC decoding."

International Conference on Post-Quantum Cryptography. Springer, Cham, 2020.

[51] Drucker, Nir, Shay Gueron, and Dusan Kostic. "QC-MDPC decoders with several shades of gray." *International Conference on Post-Quantum Cryptography*. Springer, Cham, 2020.