1176-15-333 **Sarah Arpin**, **Tyler Billingsley**, **Jun Lau** and **Angela Robinson***
(angela.robinson@nist.gov), angela.robinson@nist.gov, Gaithersburg, MD 20899. *Decoding failure analysis of iterative decoding for MDPC codes.* Preliminary report.

There is a class of public-key cryptography based on linear error-correcting codes. The decoder used during error correction directly affects the security of a code-based cryptosystem because, often, the private key is used in the process of recovering a shared secret from a syndrome. Correlations between error patterns that lead to decoding failures and the private key of a scheme have been discovered, leading cryptographers to work diligently to minimize decoding failures.

Iterative, bit-flipping decoders are not characterized by a bounded decoding radius; thus, there is an expected nonzero probability of decoding failure. Cryptographic applications require rates of decoding failures (DFR) to be less than $2^{-\lambda}$, $\lambda$ the security level. In this talk, we analyze the factors that cause decoding failures for moderate density parity check (MPDC) codes under iterative decoders and present preliminary DFR computational data for $\lambda \approx 20$. (Received January 25, 2022)