

1145-14-1409

Edoardo Persichetti* (epersichetti@fau.edu). *Reproducible Codes and Cryptographic Applications*. Preliminary report.

In this talk I will present a work on structured linear block codes. The investigation starts from well-known examples and generalizes them to a wide class of codes that we call reproducible codes. These codes have the property that they can be entirely generated from a small number of signature vectors, and consequently admit matrices that can be described in a very compact way. I will show some cryptographic applications of this class of codes and explain why the general framework introduced may pave the way for future developments of code-based cryptography. (Received September 21, 2018)