1161-11-260 **Edoardo Persichetti***, 777 Glades Road, Boca Raton, FL 33431. *LESS: designing code-based signatures without decoding.*

Code-based cryptography was born in 1978 with the intuition of Robert J. McEliece, who designed a cryptosystem based on the hardness of the Decoding Problem for random linear codes. Since then, many variants of McEliece's cryptosystem were devised, primarily in the context of encryption, always relying on the hardness of decoding. These schemes are all indirectly based on the Code Equivalence problem: in fact, the private code used in the system is hidden, by transforming it to an equivalent code, which is then released as the public code. A crucial point is that this public code is indistinguishable from random, which allows to leverage the well-known result about NP-completeness of decoding a random linear code. However, to date, no system was known to rely on Code Equivalence as a standalone problem. In this talk, we show how to build such a system, basing the security entirely on the difficulty of finding a linear isometry between codes. We then explain why this approach is promising, in particular with regards to building signature schemes, where the traditional methods have so far proved to be far from optimal. (Received August 18, 2020)