1147-11-579 **Jeffrey Hoffstein*** (jhoff@math.brown.edu), 26 Glen Drive, Providence, RI 02906, and **Joseph H Silverman**. *Short digital signatures via isomorphisms between modular lattices based on finite field isomorphisms.* Preliminary report.

The authors and several others have recently proposed a fully homomorphic encryption scheme and a signature scheme based on the observation that an isomorphism between two finite fields can be lifted to an isomorphism between related lattices. This isomorphism eliminates any Archimedean structure in one lattice from the image in the second lattice. Here we will use this concept to create a new approach to constructing signatures that is quite efficient and leads to improvements on signature size. (Received January 26, 2019)