A public key cryptosystem is said to be linearly homomorphic if its encryption functions are linear maps. Such systems are useful in electronic voting and cloud computing. We present an extended version of a linearly homomorphic cryptosystem due to the Castagnos and Laguillaumie (2015) based on the interplay between maximal and non-maximal orders of an imaginary quadratic field. In our new variant, the underlying non-maximal order is allowed to have a conductor that is a product of prime powers as opposed to a single prime as proposed in the original version. Numerical results obtained with an optimized C implementation demonstrate that this variation improves performance when large messages and exponents are used. Moreover, when compared to the linearly homomorphic cryptosystems of Paillier (1999) and Bresson-Catalano-Pointcheval (2003) at the same security levels, we found that the basic version of Castagnos and Laguillaumie is the fastest at high security levels for small messages. This is joint work with Parthasarathi Das and Michael Jacobson. (Received July 17, 2019)