1125-00-2380 **Floyd B Johnson*** (fbjohnso@mtu.edu), 310 Hancock Street, Hancock, MI 54016, and **Jie Sun**.
Reduction of ETRU to NTRU. Preliminary report.

The NTRU cryptosystem is a ring based public key cryptosystem developed in 1998 by Hoffstein et al. based over an integer modulus. The NTRU cryptosystem is faster than other popular encryption techniques such as RSA or DES and is believed to be resilient to quantum computing attacks, but has the drawback of possible decryption failure (See: Jarvis and Nevins, ETRU: NTRU over the Eisenstein integers(2015)). The ETRU cryptosystem is NTRU over the Eisenstein Integers with an Eisenstein Prime modulus of q, which are $\mathbb{Z}[\omega]/\langle q\rangle$ where ω is the third root of unity. Some attacks to find the private key include brute force, meet in the middle, and most strongly lattice methods. Traditionally ETRU is more resilient than NTRU for lattice methods and hence is considered to be stronger (Jarvis and Nevins). Presented here is the possibility of reducing the ETRU lattice to a smaller version of the NTRU lattice by constructing an explicit isomorphic mapping from $\mathbb{Z}/\langle |q|^2\rangle$ to $\mathbb{Z}[\omega]/\langle q\rangle$ then reversing this process. This mapping has restrictions on which Eisenstein prime q can be used. The repercussions of this reduction including decryption failure rate, combinatorial security, and lattice attacks will then be discussed. (Received September 20, 2016)