1147-94-598 **David Jao*** (djao@uwaterloo.ca), 200 University Ave. W, Waterloo, Ontario N2L3G1, Canada, and **Jason LeGrow**, **Christopher Leonardi** and **Luis Ruiz-Lopez**. *A subexponential-time, polynomial quantum space algorithm for inverting the CM group action.*

We present a quantum algorithm which computes group action inverses of the complex multiplication group action on isogenous ordinary elliptic curves, using subexponential time, but only polynomial quantum space. One application of this algorithm is that it can be used to find the private key from the public key in the isogeny-based CRS and CSIDH cryptosystems. Prior claims by Childs, Jao, and Soukharev of such a polynomial quantum space algorithm for this problem are false; our algorithm (along with contemporaneous, independent work by Biasse, Iezzi, and Jacobson) is the first such result. (Received January 26, 2019)