1088-94-222 **Rainer Steinwandt*** (rsteinwa@fau.edu), FAU, Department of Mathematical Sciences, 777 Glades Road, Boca Raton, FL 33431. *Implementing Binary Elliptic Curve Addition as Quantum Circuit.*

Cyclic subgroups of elliptic curves are one of the most prominent mathematical platforms in cryptography. To solve the discrete logarithm problem in such a group with Shor's algorithm, the group law needs to be realized as a quantum circuit. While the asymptotic complexity of such a computation is understood, not much work on optimizations at the circuit level is available.

For the case of binary elliptic curves, this talk discusses the implementation of point addition as a quantum circuit. A main focus is on how the choice of a particular field or curve representation affects the (gate) complexity of the resulting circuit.

The presentation is based on joint work with Brittanney Amento and Martin Rötteler. (Received February 11, 2013)