1092-94-123 **Rainer Steinwandt*** (rsteinwa@fau.edu), Department of Mathematical Sciences, 777 Glades Road, Boca Raton, FL 33431. *Applying Shor's algorithm to the discrete logarithm problem on binary elliptic curves.*

One of the main motivations for post-quantum cryptography is Shor's quantum algorithm to compute discrete logarithms efficiently. This talk discusses the complexity of realizing a discrete logarithm computation on a binary elliptic curve as a quantum circuit. The main focus is on the gate complexity (especially the number of so-called T-gates) and the circuit depth needed to realize the pertinent group arithmetic.

(This talk does not assume familiarity with quantum computing.) (Received August 05, 2013)