1148-94-320 **Hai Pham** (hpham9@fau.edu), Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, and **Rainer Steinwandt*** (rsteinwa@fau.edu), Department of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431. *On implementing the AES S-box as a quantum circuit.* Preliminary report.

Implementing Grover's algorithm to find the secret key underlying an AES-based encryption requires AES to be implemented on a quantum computer. This leads to the question of how to efficiently represent the AES S-box as a quantum circuit.

To find such a representation, different approaches have been explored. For instance, the task can be formulated as a group factorization problem, or one can try to implement the finite field arithmetic underlying the AES S-box with quantum gates. This talk discusses how existing work on logic minimization can be leveraged to devise an S-box representation involving only a modest number of qubits and non-Clifford gates. (Received February 05, 2019)