1135-VN-982 **Samundra Regmi*** (sr937857@cameron.edu) and **Parshuram Budhathoki**. *Quantum circuits for arithmetic operations over binary field.* Preliminary report.

Public key cryptography is concerned with cryptographic algorithms that require two separate keys, public and private. Public-key algorithms build on the perceived hardness of certain algorithmic problems, such as the discrete logarithm problem (DLP) and factorization problem. For classical computers these algorithms are assumed to be infeasible for suitably chosen parameters. However, Shor's algorithms offer an efficient solution of these hard problems on quantum computers. One of the critical tasks in implementing these algorithms on quantum computers is the identification (and design) of an efficient quantum circuit and underlying field arithmetic operations.

In this project, we will survey some arithmetic operations over binary field and try to optimize the design of the quantum circuits with respect to the gates, depth and qubits. (Received September 18, 2017)